AWARENESS AND TRAINING: THE INFLUENCE ON END-USER' ATTITUDE TOWARDS INFORMATION SECURITY POLICY COMPLIANCE

by

MMABATHO CHARITY SNYMAN

submitted in accordance with the requirements for
the degree of

MAGISTER TECHNOLOGIAE

In the subject

INFORMATION TECHNOLOGY

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: MISS H. ABDULLAH

February 2017

DECLARATION

Name: **Mmabatho Charity Snyman**

Student number: **50812300**

Degree: **Magister Technologiae: Information Technology**

AWARENESS AND TRAINING: THE INFLUENCE ON END-USER ATTITUDE TOWARDS INFORMATION SECURITY POLICY COMPLIANCE

I declare that the above dissertation/thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

SIGNATURE DATE

STUDENT NUMBER: **50812300**

UMI

M(I)

PAO

2001

MASTERS THESIS
PUBLISH ABSTRACT ONLY AGREEMENT
PERSONAL DATA

1. Last Name: **Snyman** First Name: **Mmabatho** Middle Name: **Charity**

2. Year of Birth (Optional) _____

3. Country of Citizenship: **South Africa**

4. Present Mailing Address
Street address:

19 Barrish Place, C/O Walter Sisulu & Barrish Lane

City	State/Province	Postal code	Country
Potchefstroom	**North West**	**2531**	**South Africa**

Future Mailing Address
Street address:

149 Meadow Street

City	State/Province	Postal code	Country
Potchefstroom	**North West**	**2531**	**South Africa**

Effective date for future mailing address (mm dd yy) **Immediately**
E-mail address: **charity.snyman@gmail.com**

Do not write in this space

Vol/Issue

School Code

Abst.

MASTER'S DEGREE DATA

5. Full name of university conferring degree, and college or division if appropriate
University of South Africa

6. Abbreviation for degree awarded
MTECH: IT

7. Year degree awarded
2017

TITLE/SUBJECT AREA

8. Enter the title of thesis. If thesis is written in a language other than English, please specify which language and translate title into English. Language of text: _____

Title: **AWARENESS AND TRAINING: THE INFLUENCE ON END-USER ATTITUDE TOWARDS INFORMATION SECURITY POLICY COMPLIANCE**

9. Subject category of thesis. Please enter four-digit code from "Subject Categories" on following page. **0984**

10. Please append an abstract of no more than 150 words describing the contents of your thesis. Your completion and submission of this form through your graduate school indicates your assent to UMI publication of your abstract. Formulas, diagrams and other illustrative materials are not recommended for abstracts appearing in *Masters Abstracts International.*

Author Signature: _____ Date: _____

DEDICATION

This dissertation is dedicated to my entire family, especially my late grandparents Crosby and Emily Snyman who inspired me to be a hardworking individual and taught me to never give up.

ACKNOWLEDGEMENT

Undertaking academic research is a long journey that requires determination and hard work. The strength to persevere when the going got tough was all because of God's Grace. "I thank you Lord for your unfailing love and the blessings you so richly bestow upon me". †

Moreover, my gratitude extents to the following people:

- Ms. Hanifah Abdullah, for being an outstanding motivator and supervisor, who kept pushing me and encouraging me to carry on. Your guidance and insightful feedback is exceptionally valued.
- My family, for their enduring support, especially my mother Grace who made herself available as always to support me in countless ways.
- My daughter Ogone, for her joviality. You kept me sane and reinvigorated when the going got tough. Love you so much my baby.
- To Fumane, you took care of us when I was focusing in this journey, without your support none of this would have been easy.
- To Wandy, thank you for assisting me whenever I needed you.
- Katlego and Reoikantse - I thank you for the support during the data collection. I couldn't have done this without you guys.
- The language editor Mrs Hendrina Krieg, thank you for your availability and support from the very beginning (proposal stage) to the very end (actual dissertation). Your assistance is truly appreciated.
- The statistician Suwisa Muchengetwa - your expertise, advice, patience and assistance is of great value.
- My Colleague Gert Van Der Merwe for all the advice, encouragement and assistance. You are one in a million.

I also wish to thank the government organisation that provided me with the opportunity to undertake this study in their setting. All the participants who took part in the study, I salute you. Finally I would like to thank UNISA and SITA for sponsoring my studies.

ABSTRACT

Research accentuates that end-users' noncompliance with information security policy (ISP) is a key concern for government just as it is for the private sector. Although awareness and training programmes are important factors impacting employees' intentions to comply with an organisation's ISP, it can be argued that there is insufficient empirical evidence to support this assertion. To address this gap, this study seeks to expand research on ISP compliance by focusing on attitudes as targets of change.

A research model based on the Theory of Planned Behaviour was proposed to illustrate the influence of ISP awareness training on end-users' attitudes towards complying with their organisation's ISP. Relevant hypotheses were developed to test the research conceptualisation. A survey and an experiment was undertaken to collect the data from a sample of 173 end-users of a single government organisation in one province. The data was captured and analysed using a Statistical Package for Social Sciences (SPSS). Furthermore, Structural Equation Modelling (SEM) was used to test whether the overall model appears to be a good fit to support the hypotheses. The reliability, validity, and model fit were found to be statistically significant, and three out of five research hypotheses were supported.

Overall this study contributes to the existing body of knowledge by providing an understanding of the methods that can be used to encourage end-users' ISP compliance behaviour through an attitudinal shift, thereby targeting end-users' attitude as a means to improve information security policy compliance. Implications of the findings are further discussed in the paper.

Keywords: Attitudes, Information Security, Information Security Policy, Awareness training, Intentions to comply, Information Security Compliance, Self-efficacy.

KEY TERMINOLOGY

Having studied the literature review it is clear that various definitions exist for information security terms, thus for the purpose of this study the following terminology can be used as a reference for discussions in the paper.

Information Security - the protection of critical characteristics (confidentiality, integrity and availability), including the systems and hardware that use, store and transmit information, through the application of policy, training and awareness programmes (Whitman and Mattord, 2013).

Information Security Policy (ISP*)* – is a vital document that sets the rules and expectations about how employees are to behave when handling information and using computer systems (Knapp and Ferrante, 2012).

Awareness Training - is described as the transition between awareness and role-based training. It is the basic and literacy training which is the bridge between awareness and role-based training and it strives to build a foundation of information security terms and concepts in an organisation's information system user population upon which later role-based training, if required, can be based (NIST, 2003).

Attitudes - A person's positive or negative feeling and or response to something (Pahnila, Siponen and Mahmood, 2007; Tipton and Krause, 2011). In the present study, attitude is defined as participants' attitude towards complying with their organisation's ISP.

Self-Efficacy - the degree to which an individual believes in their ability to enact the recommended reaction (Bandura, 1977, Fishbein and Ajzen, 2005). In the present study, self-efficacy is defined as participants' belief in their ability to comply with their organisation's ISP.

Intentions to comply- A person's readiness to perform a given behaviour (Ajzen, 2005). In the present study, Intentions to comply is defined as participants' readiness to comply with their organisation's ISP.

LIST OF ACRONYMS

IS	Information Security
ISP	Information Security Policy
CIA	Confidentiality, Integrity and Availability
NIA	National Intelligence Agency
MISS	Minimum Information Security Standards
OPM	Office of Personnel Management
IT	Information Technology
TPB	Theory of Panned Behaviour
PBC	Perceived behavioural control
STV	Subjects-to-variables
ANOVA	Analysis of Variance
CFA	Confirmatory Factor Analysis
EFA	Exploratory Factor Analysis
KMO	Kaiser-Meyer-Olkin
SD	Standard Deviation
SEM	Structural Equation Modelling
DF	Degree of Freedom
ML	Maximum Likelihood
GOF	Goodness of Fit

TABLE CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1 : Introduction

This chapter commences with the background to the research in Section 1.1. Section 1.2 focuses on the motivation of the study. The problem statement, research questions and objectives are presented in Sections 1.3 and 1.4, respectively. Section 1.5 presents a discussion on the research methodology and the research design followed in this study. The research contribution is discussed in Section 1.7. The scope of the study in terms of limitation and delineations is discussed in Section 1.8. Section 1.9 outlines the structure of the dissertation, followed by the summary of the chapter in Section 1.10.

1.1 BACKGROUND

Information has become the most vital ‘asset’ for public and private organisations and is termed ‘information asset’ or ‘intellectual asset’ (Sung and Su, 2013). In order for this information to have business value, it must be accurate, complete and timely (Raggad, 2010). Sung and Su (2013) state that it is particularly important to protect this asset (information) to ensure its confidentiality, integrity and availability (CIA), since managing the security of information is as important as managing the core business of the organisation. According to Safa, Von Solms and Furnell (2015), hackers use different methods to change the CIA of information for their own benefits, while users intentionally or through negligence are a great threat for information security.

To protect critical information assets, organisations often deploy technical tools such as firewalls and comprehensive monitoring systems. Although these tools offer technical solutions, they are rarely sufficient in providing total protection of organisational information resources (Vance, Siponen and Pahnila, 2012). According to Whitman and Mattord (2013), in order to protect information and its related systems, organisations must implement additional strategies such as policies and procedures.

Moreover, Bulgurcu, Cavusoglu and Benbasat (2010) and Ng, Kankanhalli and Xu (2009) suggest that one of the strategies that organisations use in the implementation of information security (IS) is the information security policy (ISP).

The ISP is a vital document that set the rules and expectations about how employees are to behave when handling information and using computer systems. Furthermore, the ISP guides the corporation, its employees, customers and vendors in securing their information (Knapp and Ferrante, 2012).

According to Bishop and Nascimento (2016), in order to successfully implement ISPs, users must make critical security decisions to comply with ISPs. Moreover, Bulgurcu *et al*. (2010) suggest that employees who comply with the information security rules and regulations of the organisation are the key to strengthening information security. Likewise, Safa *et al.* (2015) accentuate that there is an increased need to accommodate the human factor in IS, as the technical aspects cannot solely guarantee a secure environment. Moreover many organisations recognise that their employees, who are often considered the weakest link can also be great assets in the effort to reduce risks related to information security (Rastogi and Von Solms, 2011; Knapp and Ferrante, 2012). An understanding of methods that can influence behaviour is thus crucial for organisations that want to leverage their human capital (Bulgurcu *et al*., 2010).The following section provides the background to this study by highlighting the motivating factors.

1.2 RESEARCH MOTIVATION

The world has changed dramatically during the last few years, with profound implications for society and government. Likewise (Rossi, 2016) indicates that "attack vectors continue to change and security breaches are becoming more frequent and sophisticated than ever". According to (Grimes, 2015), most of the threats towards information security in the yesteryears were malware programs designed by adolescents male pranksters, to format disks or erase files as well as to annoy people. However, nowadays most malware is created to steal money or trade secrets by professional hackers. Furthermore, (Grimes, 2015) accentuates that Advanced Persistent Threats working on behalf of foreign governments are the new norm.

According to Marano, Rokas and Kochenburger (2016), a government's national security concerns include maintaining the confidentiality of information, protecting infrastructure and preventing cyber-attacks that could paralyse the country.

Moreover, Sharma and Gupta (2009) propose that any organisation should have interest in protecting its assets against undesired events threatening the CIA of information.

Like any other government organisation in the world, the Republic of South Africa has to serve and protect its own interests. Hence the National Intelligence Agency (NIA) has a statutory responsibility to protect the interests of the nation through counter-intelligence measures such as the Minimum Information Security Standard (MISS) to guide government departments when drawing up comprehensive security policies in order to deal with various aspects of information security (Basani, 2012). Likewise, Shaw (2012) emphasises that organisations must be guided by their own policies regarding information security in response to statutory and regulatory commitment and the risks facing organisations.

However, Bulgurcu *et al*. (2010) argue that, while creating guidelines and policies is an essential starting point, it is not enough to ensure employees' compliance with them. Puhakainen and Siponen (2010) indicate that employee non-compliance with ISPs is a key concern for organisations. Similarly, Boshoff (2010), Mavetera and Makhudu (2012) and Siponen, Mahmood and Pahnila (2014) suggest that the major threats to IS are constituted by ignorant and careless employees who do not comply with organisational ISPs. According to Mavetera and Makhudu (2012), most employees are not aware of ISPs implemented in their organisations; the few that are aware are often let down by their organisations' failure to implement security training programs for educating employees of the right security procedures. Likewise, Rastogi and Von Solms (2011) suggest that users may be aware of the existence of policy documents, but seldom make any effort to read them and thus do not know the contents.

Although emerging research on the human perspective regarding information security shows that employee compliance to information security policies is a challenge, awareness and training are the most commonly suggested ISP approaches in literature. Herold (2010) suggests that training is one of the most effective methods by which an organisation can safeguard its information assets. Moreover, the (ISO/IEC 27002, 2013) indicates that all employees should receive

awareness and training updates relating to the organisational policies and procedures as part of the code of practice for managing information security.

Merhi and Midha (2012) suggest that security training has been shown to be an important factor that impacts employees' intentions to comply with the organisation's security policies. Other authors suggest that information security managers should prioritise their efforts to focus largely on policy awareness, as this had the largest impact on effectiveness in their studies (Bulgurcu, 2010; Puhakainen and Siponen, 2010; Al-Omari, Deokar, El-Gayar, Walters and Aleassa, 2013; Knapp and Ferrante, 2012).

Although the need for awareness and training is clear, other researchers suggest that previous research examining security awareness effectiveness has shown inconclusive results (Wolf, Haworth and Pietron, 2011). Furthermore, few of the existing studies regarding training to promote ISP utilise theory to explain which learning principles affect user compliance and do not offer empirical evidence of their practical effectiveness (Puhakainen and Siponen, 2010).

According to Puhakainen and Siponen (2010), information security training and education approaches for compliance have largely remained theoretical and anecdotal. Moreover, Ng *et al*. (2009) indicate there is a lack of research on behavioural information security and theoretical models which explain how awareness training affects behaviour. Specifically, there is a shortage of research demonstrating the practical effectiveness of information security awareness training. Furthermore, D'arcy, Hovav and Galletta (2009) indicate that the direct and indirect roles of information security awareness on an employee's compliance behaviour have not yet been studied.

Despite these arguments, it is suggested that there is a clear need to ensure that users are made aware of ISPs in their organisations and are properly trained in terms of ISPs (Haeussinger, 2013). Furthermore, Al-Omari *et al*. (2013) suggest that awareness and training ensure that users cannot misuse or misinterpret policies, which thereby ensure their effectiveness.

Additionally, Waly, Tassabehji and Kamala (2012) suggest that there is a scope for research on the factors that influence user behaviour and attitudes toward

information security. Likewise, Safa, Von Solms and Furnell (2016) calls for research that focuses in learning perspectives that might well be interesting and effective in complying with ISPs. Therefore, this study aims to empirically investigate the influence of ISP awareness training on end-user attitude towards complying with an organisations' ISP.

1.3 PROBLEM STATEMENT

From the above discussion, a case can be made for awareness and training as crucial to promote desired user behaviour towards information security. According to Bulgurcu *et al.* (2010), ensuring information security awareness can directly and indirectly alter employees' belief sets about compliance with the ISP, suggesting that creating a security-aware culture within the organisation will improve information security. The (NIST, 2009) emphasises that the fundamental value of information security programmes is that they set the stage for awareness and training by bringing about change in attitudes, which should influence the organisational culture. However, despite the importance of information security awareness, there is a paucity of empirical studies that analyse the impact of information security awareness on information security behaviour (Bulgurcu *et al.*, 2010).

According to Puhakainen and Siponen (2010), there is a lack of research on behavioural information security and theoretical models that explain the way in which awareness training affects behaviour. Other authors have called for further research to demonstrate the value and the significant contribution that shows information security awareness efforts to be beneficial (Bulgurcu Cavusoglu and Benbasat, 2009; Bulguru *et al*., 2010). Ng *et al*. (2009) state that there are relatively few research studies on security behaviour of computer users and how behaviour can be modified to practice security countermeasures.

The focus area of this study is therefore to propose and empirically validate a model in order to investigate the significance of ISP awareness training in influencing end-user attitudes towards complying with their organisations ISP.

1.4 RESEARCH QUESTIONS AND OBJECTIVES

The main objective of this study is to investigate the influence of ISP awareness training on end-user attitudes towards complying with their organisations ISP. The main research objective is explored by investigating the following research sub-objectives:

- *To determine the current end-users' level of ISP awareness training and ISP compliance behaviour.*
- *To assess the influence of ISP awareness training on end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP.*

To achieve these sub-objectives, this study will address the following research questions:

- *What is the current end-users' level of ISP awareness training and ISP compliance behaviour?*
- *How does ISP awareness training influence end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP?*

1.5 RESEARCH METHODOLOGY

This section provides an overview of the research methodology used to achieve the objective of this study. A detailed research methodology is discussed in Chapter 5.

1.5.1 Research Approach

To accomplish the research objective, this study adopted Creswell's (2014) framework for research. According to Kumar (2014), a study is classified as quantitative if one wants to quantify the variation in a phenomenon and the analysis is geared to ascertain the magnitude of the variation. Moreover, Creswell (2014) suggests that a quantitative research approach allows a researcher to test a theory by specifying narrow hypotheses to collect data to support or refute the hypotheses. In the context of this study, a model based on the theory of Theory of Planned Behaviour (TPB) is proposed to test or refute the hypotheses.

1.5.2 Research Paradigm

The researcher used a positivist paradigm as the blueprint to guide the study. The rationale being positivism assumptions are more associated with quantitative research than qualitative research, as the problems studied by positivists reflect the need to identify and assess the causes that influence the outcomes (Creswell, 2014), just as the current study aims to investigate the influence of ISP awareness training on end-users attitudes toward ISP compliance.

1.5.3 Research designs

Two research strategies of enquiries that invoke the positivist paradigm and are associated with quantitative research are adopted in the current study as follows:

- A **descriptive** study is undertaken to provide a picture of the end-users' level of ISP awareness training and their current compliance behaviour;
- Whilst the **explanatory** study is undertaken to assess the influence of ISP awareness training on end-users' attitudes toward ISP compliance by proposing and empirically evaluating a model based on the TPB.

According to Remler and Van Ryzin (2011), research that is descriptive aims to describe the world and how things are. Whereas explanatory (causal) research aims to provide an explanation of how things would be different if something is changed (cause effect relationship). Thus the current study undertakes both a survey and experimental designs. The survey is conducted prior to the experiment to identify the characteristics and culture of the population in terms of compliance behaviour and level of ISP awareness training, so that inferences can be made about the information security practices of the organisation. According to Creswell (2014), surveys are used for the purpose of generalising from a sample to a population so that inferences can be made about some characteristic, attitude or behaviour of a population.

Additionally, the experiment design is conducted to test the theory of ISP awareness training influencing end-users' attitudes toward complying with their organisation's ISP. According to Leary (2012), an experimental design is described as a research design that is designed to test whether certain variables cause changes in

behaviour. A two-group, random-selection, pre-test *and* post-test experimental design was used to measure the influence of ISP awareness training on end-users' attitudes toward ISP compliance. Since experimental designs seek to determine if a specific treatment (interventions) influences an outcome (Jacobsen, 2012), the experimental group was exposed to an information security policy video and a brief presentation of security basic and literacy training, with the objective of comparing the outcomes in participants assigned to an intervention and the control group. This customised approach was targeted to end-users with appropriate content (e.g. a subset of behaviours based on the requirements of their organisation's ISP). The procedure and design of the experiment is presented in Section 6.2.

1.5.4 Research methods

The specific research methods applied in this study are discussed as follows:

- **Data collection methods**

The primary source of data collection for this study was questionnaires for the survey and pre-test *and* post-test questionnaires for the experiment. According to Kumar and Phrommathed (2005), questionnaires provide a standard format on which facts and or attitudes can be recorded and easily processed. The questionnaire was used to assess the current compliance behaviour and the level of end-users' ISP awareness training in order to determine the organisation's culture regarding ISP compliance. Subsequently, the data for the experiment was collected to compare the pre-post test to determine if ISP awareness training does influence end-users attitudes toward complying with their organisation's ISP.

Although items that have been tried and tested by extant research were used in order to maximise the instrument's reliability with respect to the items used in the survey questionnaire and the pre-test *and* post-test questionnaire, the research instrument was tested for reliability and validity in the context of this study. The results are presented in Section 6.4. The advantage of using items from previous research is that they are already verified and thus improve the reliability of results (Kim, Yang and Park, 2014).

- **Data analysis methods**

According to Oates (2006), quantitative data analysis is mainly used for the type of data generated by surveys and experiments. Thus the findings of this study were analysed using statistical analysis to determine the level of ISP awareness training and compliance behaviour of end-users, as well as to determine the effect of the intervention. Furthermore the services of a statistician were used to analyse the data.

1.6 POPULATION AND SAMPLING

Stangor (2011) indicates that the entire group that the researcher desires to learn about is known as the population, and the smaller group of people who actually participate in the research is known as the sample. The population for this study was a government organisation located in the North West province. Although a probability sampling technique would have been preferred, the convenience sample was the only sampling technique that could be used to collect the data, since the organisation granted permission to conduct the study on condition that a list of computer users is not provided for the research to assure anonymity. Regardless of the likelihood of the sample being representative is low in convenience sampling, Oates (2006) and Welman, Kruger and Mitchell (2005) suggest that this problem is less important where there is little variation in the population and sample. In this context, this study is concerned with end users of a government organisation, thus the participants were end users of a government organisation.

1.7 RESEARCH CONTRIBUTION

Although information security awareness, policies and behavioural models such as the TPB have been studied extensively, there is a paucity of research rooted in end-users' conscious behaviour (e.g. attitude). According to Tipton and Krause (2012), attitudes as targets of change can equally influence ISP behaviour.

This study aims to contribute to the existing body of knowledge by providing insights into the role of ISP awareness training on end-users' attitudes toward ISP compliance and its practical effectiveness to appropriate behaviour. Thereby enabling information security practitioners to structure ISP awareness programmes

in a way that changes both the perception and ISP conscience behaviour of end-users, so that when a security event happens, the appropriate response will occur.

Moreover, previous research accentuates the fact that research that contributes to the effectiveness of awareness training will ultimately benefit organisations and will allow them to focus on techniques that improve their employees' intentions and eventually encourage end-user security behaviour towards a more favourable state (Herath and Rao, 2009; Bulgurcu *et al*., 2010; Ifinedo, 2014).

1.8 LIMITATIONS AND DELINEATIONS

The main limitations and constraints of this study are as follows:

- The focus of this study was on attitudes as targets of change, and the main aim of the study was to assess the influence of ISP awareness training on end-users' attitudes toward ISP compliance. In order to assess this theory, a model based on the TPB was used. Three constructs known to affect behaviour in the TPB are: attitudes, subjective norms and perceived behavioural control. However, subjective norms were excluded in this study as they have been found to produce low meta- analysis when used with the other TPB constructs. According to Ajzen (2005), not all TPB constructs need to be significant to successfully explain intentions and behaviour, as the relative importance of the three constructs is likely to change depending on the area of interest.
- The other limitation is with regard to the learning continuum used in this study. There are three levels of learning in the (NIST, 2009) learning continuum, namely: awareness, training and education. The focus of the study was only on the awareness and awareness training level, thus role-based training and education were not considered as they relate to one's roles and responsibilities relative to IT systems and the skills needed to further the IT security profession.
- One more limitation relates to the sampling procedure, since the organisation granted permission to conduct the study on condition that a list of end-users is not provided for the research to assure anonymity, the sample was not chosen at random. However Welman *et al.* (2005) suggests that non-

representativeness is less important when there is little variation in the population and sample, thus in this study participants were selected by means of a well-defined criterion (i.e. the sample was end-users of a government organisation). Nevertheless, generalisations from the sample obtained, to the population being studied can still be criticised since the sampling frame is unknown.

- The following delineation is applicable: The scope of this study is delimited to a government organisation in the North West province. The organisation has offices in three locations, namely Mafikeng, Potchefstroom and Zeerust. As a result of this delimitation the results of this study cannot be generalised to other government organisations, provinces or the private sector. However the results are applicable for the population from which the sample studied was taken.

1.9 DISSERTATION LAYOUT

This dissertation consists of eight chapters, which are outlined as follows:

1.9.1 Chapter 1: Introduction

The chapter provides the background of this study. The motivation and contribution of this study are introduced in this chapter, as are the problem statement and the research objectives.

1.9.2 Chapter 2: Information Security Background

This chapter provides information security background and discusses the significance of ISPs. Areas covered in this chapter include an overview of information security practices in terms of international IS standards and the activities initiated by the South African government for information security.

1.9.3 Chapter 3: Information Security Education

Chapter 3 provides a background overview of information security learning and the benefits it has on desired information security behaviour.

1.9.4 Chapter 4: Theoretical Framework

This chapter provides the theoretical framework underpinning this study and discusses the proposed model and the assumed hypotheses to determine the influence of ISP awareness and training on end-users' attitudes toward compliance behaviour.

1.9.5 Chapter 5: Research Methodology

Chapter 5 presents the research design and approaches, undertaken in this study to test the objectives introduced earlier in the chapter. Ethical considerations are also discussed in this chapter.

1.9.6 Chapter 6: Data collection and Analysis Methods

The chapter discusses the data collection and data analysis methods undertaken in this study to answer the research questions. This chapter also covers the construction of the research instrument and its validity and reliability.

1.9.7 Chapter 7: Research results and Interpretation

Chapter 7 presents and interprets the findings of the data collected to substantiate the proposed theoretical model.

1.9.8 Chapter 8: Conclusion

This chapter concludes the study by providing the outcome of the assumptions made to test the theory that was proposed. Implications and recommendations for future research are also presented in this chapter.

1.10 SUMMARY

The purpose of this chapter is to provide an overview of what this study entails. The motivation and background this study is based on is also discussed in this chapter. The next chapter presents the literature review to discuss information security background and practices.

Chapter 2 : Information Security Background

2.1 INTRODUCTION

In order to demonstrate the importance and focus of this study, this chapter outlines the background of information security (IS) in Section 2.2, and discusses information security policy and compliance in Section 2.3, followed by a comparison of information security in the public and private sectors in Section 2.4. Section 2.5 provides a review of international standards relating to information security, whilst information security initiatives taken in the country where this study was undertaken is discussed in Section 2.6. The chapter then concludes with a summary in Section 2.7.

2.2 BACKGROUND OF INFORMATION SECURITY

Public and private sector enterprises today are highly dependent on information systems to carry out their mission, vision and business functions (Ngomeni and Grobler, 2009). Due to this dependency, a number of Information Security (IS) incidents that organisations encounter have increased globally (Pahnila *et al*., 2007; Sharma and Gupta, 2009; Knapp and Ferrante, 2012). There are frequent major data breaches in industry and government agencies, such as the 2011 Citibank incident where hackers accessed millions of their credit card customer accounts (Chan and Gogoi, 2011) and the cyber-attack on the United States Office of Personnel Management (OPM) server where 4.2 million federal employees' data (including security clearance forms and sensitive information about intelligence and military personnel) was stolen by hackers (Johnson 2015; Davis 2015).

Evidence from literature suggests that the reason why information security incidents continue to plague organisations is the variety of threats and weaknesses infiltrating security controls. Consequently, a critical need for businesses and governments to strengthen information security programmes to combat these threats has been suggested in literature (Knapp and Ferrante, 2012; Whitman and Mattord, 2013; Sung and Su, 2013). Likewise, Sung and Su (2013) propose managing the security of information, as it is as important as managing the core business of an organisation.

According to Whitman and Mattord (2013:4), information security is “the protection of critical characteristics (confidentiality, integrity and availability), including the systems and hardware that use, store and transmit that information, through the application of policy, training and awareness programmes”. Moreover, Tipton and Krause (2012) emphasise the importance of minimising the threats to the confidentiality, integrity and availability (CIA) of data and computing resources. Likewise, Whitman and Mattord (2013) and Sung and Su (2013) indicate that the protection of information is concerned with three main principles (CIA), which are the primary goals of information security. Figure 2-1 depicts the CIA triad adapted from Tipton and Krause (2012).

Figure 2-1: CIA Triad from (Tipton and Krause, 2012)

2.2.1 Principles of information security

Whitman and Mattord (2013) explain the CIA triad as follows:

Confidentiality: ensures that only those with the rights and privileges to access information are able to do so. Information has confidentiality when it is protected from disclosure or exposure to unauthorised individuals or systems. When unauthorised individuals or systems can view information, confidentiality is breached.

Integrity: Information has integrity when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data.

Availability: enables authorised users to access information without interference or obstruction and to receive it in the required format.

In addition to the CIA triad, Sterwart, Chappel and Gibson (2015) suggest that one needs to consider a plethora of other related security concepts and principles when deploying a security solution. Therefore, the following section discusses other proposed information security principles relating to employees in an organisation in order to secure organisation information.

2.2.2 Other important information security principles

Sterwart *et al*. (2015) discuss other information security principles as follows:

- **Identification** - Prior to performing any activities on an organisation's network, individuals must first introduce themselves (identification) and prove that they are who they say they are (authentication). The reason for this process is that the computer must be able to, at any time, ensure that only legal or authorised entities are using it and it must also be able to enforce accountability. The first step towards identification on a computer system is for a user to provide valid user identification (user ID) or swiping a smart card. Without identification the system has no way of correlating an authentication factor with the user, to verify the identity of the user before access to controlled resources is granted.
- **Authentication** - authentication verifies that the username does indeed, legally, belong to a user. This is to further ensure that only legal users and not impostors obtain access to the system and its resources. One can do this by providing a password, a token card or smart card, or biometrics. These mechanisms can be used together.
- **Authorisation** - The aim of authorisation is to ensure that only legitimate users can obtain access to computing facilities, and that only allowable and legitimate actions will be performed. In order to achieve this, one needs to control access on the network.
- **Auditing –** is a programmatic means by which a user's actions are tracked and recorded for the purpose of holding the user accountable for their actions whilst authenticated on the system. Furthermore, the audit trails created by the system event logs are needed to identify malicious actions by users,

attempted intrusions and system failures. Auditing also reconstructs events to provide evidence for prosecution and produce problem reports and analysis.

- **Accountability** - determines the actions of the users and system resources on the network. Thus an organisation's ISP can be properly enforced only if accountability is maintained. Accountability is established by linking a user to the activities of an online identity through the security services and mechanisms of auditing, authorisation, authentication and identification. Moreover, to enable accountability, it is suggested that one must be able to legally support the security efforts in order to hold a user accountable for actions linked to their user account.
- **Non-repudiation** - proves beyond a reasonable doubt that a transaction, message or data originated from a specific user (source) and terminated at a specific user (destination). This can be proven by the use of digital certificates and digital signatures. The advantage of this mechanism is that the user cannot deny sending or receiving a message.

Chakraborty and Raghuraman (2013) emphasise that well-established core principles of information security are Confidentiality, Integrity and Availability (CIA triad). Moreover, authentication enforces confidentiality; authorisation enforces integrity and non-repudiation helps enforce availability (Chakraborty and Raghuraman, 2013). According to Whitman and Mattord (2013), CIA does no longer adequately address the constantly changing information technology environment, as the threats to the CIA of information have evolved into a vast collection of incidents such as accidental or intentional damage, theft, unauthorised modification or other misuses from human or non-human threats. The following section therefore discusses the types of threats concerning CIA of information.

2.2.3 Threats to CIA of information

As discussed above, there are different types of threats infiltrating the CIA of information. As a result the importance of IS has increased and this is illustrated by the growing number of IS incidents that organisations encounter (Peltier, 2014). These incidents are classified as internal and external threats ranging from errors that can destroy information integrity, to a hacker sitting up until all hours of the night finding ways to steal the company's secrets, (Peltier, 2014). Ngoma (2012) and

Sommestad, Hallberg, Lundholm and Bengtsson (2014) discuss external and internal threats as follows:

2.2.3.1 External threats:

- **Malicious codes (viruses, worms, Trojan horses etc.):** Computer programs that have the capability to automatically replicate themselves across systems and networks.
- **Natural disasters:** Damage to computing facilitates or data resources caused by phenomena such as earthquakes, floods, or fires; resulting in loss of the physical facility or the supporting infrastructure.
- **Spam e-mails (opening):** Unsolicited e-mail.
- **Hacking incidents:** The penetration of organisational computer systems by unauthorised outsiders, who are then free to access and manipulate data.

2.2.3.2 Internal threats:

- **Installation /use of unauthorised hardware, peripherals or software**: Information systems, especially financial systems, are vulnerable to individuals who seek to defraud an organisation.
- **Abuse of computer access controls**: The deliberate abuse of systems and the data contained therein by users of those systems.
- **Physical theft of hardware /software**: Theft of valuable hardware, software and information assets.
- **Errors and omissions:** The accidental destruction or incorrect entry of data by computer users.
- **Deliberate damage by displeased employees**: Disgruntled employees may seek revenge by damaging their employees' computer systems.
- **Use of organisation resources for illegal communications or activities such as porn surfing and email harassment**.

According to Crossler, Johnston, Lowry, Hu, Warkentin and Baskerville, (2013), more information security breach incidents are caused by intentional or unintentional actions of insiders than by outside hackers. The insider threat is an authorised, non-technical user of the system who has been around long enough to determine which actions would cause a "red flag" (Peltier, 2014). Likewise, Waldo and Marthias (2016) indicate that employees are the weakest link in an organisation's defence

against external information security threats. According to a study by the Ponemon Institute and Raytheon Release New Study on the Insider Threat (2014), 88% of IT experts suggest that the risk of insider threats will increase in the next coming years. Consequently, Peltier (2014) accentuate that the various types of threats makes it very difficult to establish and maintain information security.

Furthermore, Whitman and Mattord (2011) indicate that the constant evolution of IS threats has prompted for the development of a more robust intellectual model that addresses the complexities of the current information security environment. This model is depicted in Figure 2-2 and is an expansion of the CIA triangle. It consists of a list of critical characteristics of information, which are described in the next section.

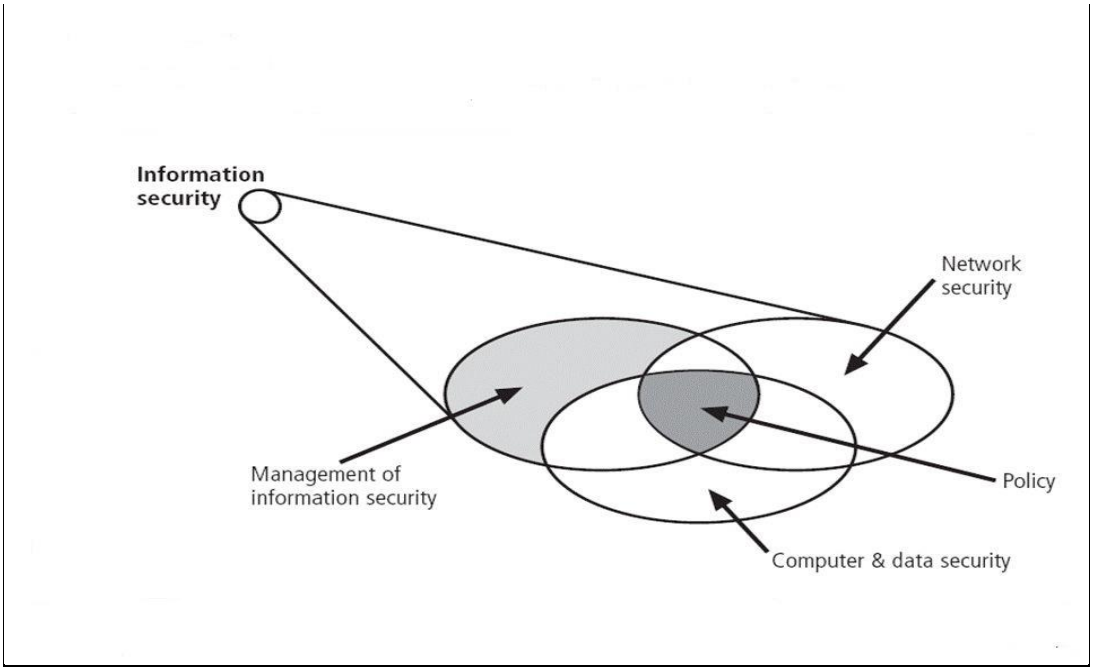


Figure 2-2: Components of Information Security (Whitman and Mattord, 2011)

Whitman and Mattord (2011) suggest that information security includes the broad areas of information security management, computer and data security and network security, with the policy as the overlapping area of the information security components. According to Whitman and Mattord (2011), the meaning of policy is dependent on its context, e.g. government organisations discuss ISP in terms of national security and national policies to deal with foreign countries; whilst in general an ISP is a set of rules that protect an organisation's assets. Moreover, Shaw (2012)

defines an ISP as a guide to an organisation and its employees in the use of information security. Therefore the following section discusses ISPs.

2.3 INFORMATION SECURITY POLICY

Ngobeni and Grobler (2009) describe the ISP as the cornerstone of information security effectiveness, as it is the document that regulates how an organisation will manage, protect and distribute its sensitive information. Moreover, the (ISO/IEC 27002, 2013) indicates that the objective of the ISP is to provide management with direction and support in accordance with business requirements and regulations when dealing with information security.

According to Sharma and Gupta (2009), the purpose of the ISP is to establish an organisation-wide approach to prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of organisation's data, networks and computer systems; in order to define mechanisms that protect the organisation from its legal and ethical responsibilities. However, Rastogi and Von Solms (2011) argue that the effectiveness of information security policies and control measures organisations depends to a large extend on secure actions by end-users. It is also recognised that employees can help organisations safeguard IT resources by performing beneficial acts. To encourage such acts, organisations often put together an ISP that stipulates what roles employees should play (Bulgurcu *et al*., 2010). Similarly, Peltier (2016) suggests that ISPs establish the behaviour expected of all personnel granted access to an organisation asset. Moreover, recent studies such as Bulgurcu *et al*. (2010) and Ifinedo (2012) signify the pertinence of employees' compliance with their organisation's ISP, thus the following section discusses guidelines for effective ISPs.

2.3.1 Guidelines for an effective ISP

According to Ngobeni and Grobler (2009), a well-written ISP must satisfy the needs of the organisation, and must be practical and enforceable. Moreover, Whitman and Mattord (2013) argue that a policy is only enforceable if its properly designed, developed and implemented using a process that assures repeatable results. One effective approach proposed by the authors for policies to be effective is that is policies should be:

- Developed using industry-accepted practices
- Distributed using appropriate methods
- Read by all employees
- Understood by all employees
- Formally agreed to by act or affirmation
- Uniformly applied and enforced.

2.3.2 Contents of the Information Security Policy

According to Peltier (2016), information security policies are used to introduce the concepts of what is expected of all employees when using enterprise assets, and what non-compliance can lead to. In their study, Ngobeni and Grobler (2009) collected ISPs from four IT-related governmental organisations and reviewed them based on the characteristics of what a good policy should contain. Although the list is not all-inclusive, it is relevant to the current study as the current research studies a government organisation to determine the influence of ISP awareness training on end-users' attitudes toward ISP compliance. The following contents of an ISP as reviewed by Ngobeni and Grobler (2009) are indicated:

- **Access control.** To describe rights and permissions and to whom these privileges should be granted with regards to accessing a particular resource within the organisation.
- **Data classification and control.** Data need to be classified according to its level of sensitivity to assist the organisation in determining the extent of security needed. Data can be classified as top secret, secret, confidential, proprietary, sensitive, private or public use (Whitman and Mattord, 2011).
- **Risk assessment.** The organisation's information systems need to be assessed to identify vulnerabilities/threats/risks that can affect the confidentiality, integrity and availability of the key information assets.
- **Password and user ID management:** the policy should stipulate the rules for how to compose and manage passwords.
- **Encryption and digital signatures:** addresses the need for encryption and digital signatures as means to achieve data security within the organisation.

- **Instant messaging, PDAs and smart phones:** the policy must provide procedures and regulations regarding the use of Instant Messaging, PDAs and smart phones within the corporate environment.
- **Security awareness and training.** The policy needs to facilitate compliance by employees regarding the organisation's stated rules and procedures.
- **Data privacy management for employees and customers:** The policy needs to address the privacy relationships between collection, storage and dissemination of information.
- **Corporate Governance:** the policy should discuss the procedures by which a business is operated, regulated and controlled. It should also discuss the internal factors defined by the officers, the constitution of the company and external forces such as consumer groups, clients and governmental regulations.
- **Electronic mail, viruses, malicious code protection and social engineering attacks, including phishing scams: t**he policy should address the protection of the organisation's networks and information systems from malicious codes and social engineering. The methods of creating, transmitting or storing primary text must also be stipulated.
- **Identity theft:** addresses the prevention of identity theft and related attacks.
- **Network security:** addresses the protection of the network and its services, unauthorised modification, destruction and disclosure of information, and assuring that the critical network functions correctly and is available from at all times.
- **Firewalls and Intrusion Detection Systems (IDSs):** The policy should address the use of firewalls to prevent unauthorised internet users from accessing the organisation's private networks, and to prevent organisation's users from accessing unauthorised internet content. Furthermore, methods to detect malicious network traffic and computer usage should also be addressed.
- **Communication security, including telephones and fax machines:** The policy should cover issues related to communication security, such as telephone, fax equipment and email.

- **Website and e-commerce security:** the policy should describe how to protect the organisation's website against security weaknesses such as SQL injections, Denial of Service attacks and spam relaying.
- **Security in third party contracts, including outsourcing and offshoring of IT project:** the policy should address security in its infrastructure and assets, whilst complying with regulations applicable to third party contracts.
- **Retention and disposal of documents:** the policy should clearly address the destruction and retention of documents.
- **Incident response and contingency planning:** issues concerning how an organisation will respond quickly and effectively to a system or network security breach should be indicated, disaster and business continuity planning should also be addressed by describing the organisation's immediate actions in response to unexpected business interruptions or disasters.
- **Telecommuting and mobile equipment:** telecommuting and the use of mobile equipment as a means to protect organisational assets outside the perimeters of the organisation should be addressed.

With regard to ISPs, Ng *et al*. (2009), Bulgurcu *et al*. (2010) and Ifinedo (2011) maintain that users have to make a conscious decision to comply with the organisation's rules, guidelines and requirements as laid out in their security policies and to adopt computer security behaviour, in order for information security to be effective. Therefore the next section discusses ISP compliance.

2.3.3 ISP Compliance

Employee and user compliance has been studied extensively in IS research. Although literature suggests that employee compliance can be achieved through education and training or fear of appeals and deterrence (Herath and Rao, 2009; Siponen and Vance, 2010; Merhi and Midha, 2012), employees' compliance with information security policies is still reported as a key information security problem for organisations (Puhakainen *et al*., 2010; Siponen et.al 2014). Bulgurcu *et al*. (2010) argue that, while creating guidelines and policies is an essential starting point, it is not enough to ensure employees' compliance.

According to Sharma and Gupta (2009), enforcement of policies is important, because if information security breaches occur and they are not addressed,

employees might think that policies can be safely ignored, thus increasing the risk that real damage will be done the next time an incident occurs. Therefore, an understanding of what factors motivate employees to comply with their organisations' ISPs is central to helping information security managers diagnose the deficiencies in their information security management efforts and in providing them with ways to solve the behavioural issues in information security management (Sharma and Gupta, 2009).

While Siponen and Vance (2010) suggest that neutralisation techniques by means of deterrence only enables employees to violate information security controls by temporarily relieving them from fear of punishment, D'Arcy *et al*. (2009) found that perceived severity of punishment was increased by security policies, monitoring and awareness programmes, which resulted in reduced intentions to abuse computer resources. On the other hand, Tipton and Krause (2011) propose employee motivation and rewards and recognition as a means to discourage employees from attempting to bypass security controls.

However, Ng *et al*. (2009) accentuate that, in order for security to be effective, users have to make a conscience decision to comply with the organisation's security policies and adopt computer security behaviour in order to minimise the probability of costly IS incidents. Knapp and Ferrante (2012) propose that organisations should be highly motivated to communicate, enforce and maintain security policies. According to Barton (2014), employees are more likely to comply with ISPs they perceive as fair. To improve employee compliance behaviour with IS controls, it is suggested that the desired beliefs such as attitudes are shaped (Bulgurcu *et al*., 2010). Furthermore, Rastogi and Von Solms (2011) suggest that organisations should document their ISPs and controls in order to conduct awareness and training campaigns for their end-users. According to Puhakainen and Siponen (2010), awareness of policies is needed by all individuals in an organisation to ensure that policies are well understood. Moreover, since the advent of costly computer viruses the world is becoming more regulated, with new laws specifying how information must be handled and safeguarded; thus making security policy operational is no longer a nice-to-have, but a must-do for any private and public organisation (Whitman and Mattord, 2011). The following section therefore discusses information security practices in private and public sectors.

2.4 THE DIFFERENCE BETWEEN PRIVATE AND PUBLIC SECTORS

As indicated earlier in this chapter, both private and public sectors have had equally disastrous data breaches to date, hence both sectors have a growing scale of technology which often facilitates costly people and process-faulted information security breaches (King and Hart, 2009). Furthermore, it is suggested that the difference between private and public sectors becomes clearer when we look at levels of capability maturity in the supporting infrastructure and capacity (ISO 27001, 2013). When comparing both sectors, it is believed that the public sector is head and shoulders above and beyond anything the private sector is doing, or has done in this regard, from the early foresight and initial sponsorship of the development of ISO 27001.

Ritchey (2010) indicates that the private and public sectors have quite a bit in common. For instance, when financial resources are scarce, local government entities are said to be looking more closely at public-private partnerships as a means of tapping the expertise and economic power of the private sector to make large projects that might otherwise not happen possible. Moreover, it is revealed that many security executives within the public sector say that they could not do without their private sector counterparts, as the ability to work closely with stakeholders throughout their respective security communities and the cooperation often allow them and their security partners to improve procedures and share best practices (Ritchey, 2010). Likewise, Raduege, Jr. (2013) also suggests that the public and private sectors need to work together to protect critical assets with confidence and trust to help manage known risks, and getting ahead of those that are not known. The two primary areas of concern stipulated by the report are:

- Crafting a cyber-security framework that addresses risks across government and industry, and
- The concept of enhanced public/private information sharing and developing standards.

Subsequently, different standards or guidelines are available to adapt for organisational use in response to compliance with statutory and regulatory requirements (Shaw, 2012). Thus the following section discusses the standards regarding information security.

2.5 INTERNATIONAL INFORMATION SECURITY STANDARDS

According to Siponen and Willison (2009), international information security standards play a key role in managing and certifying organisational information security. It is further recognised that established international standards are a good starting point for implementing the ISP to improve the information security in an organisation (Siponen and Willison, 2009; Susanto, Almunawar and Tuan, 2012). Susanto *et al*. (2012) further suggest that standards or benchmarks regulating governance over information security are mandatory. Hence private and government organisations developed standard bodies whose function is to setup benchmarks, standards and legal regulations on information security to ensure that an adequate level of security is preserved, and that best practices are adopted in an organisation. The focus in this study is on the standards and initiatives affecting the information security environment. Therefore the standards developed for information security are briefly discussed as follows:

2.5.1 ISO/IEC 27001:2013 (Information Security Management System-Requirements).

ISO/IEC 27001:2013 is the first revision of ISO/IEC 27001:2005, and specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature. The difference between ISO/IEC 27001:2013 and ISO/IEC 27001:2005 is that there are no duplicate requirements, and the requirements are phrased in a way that allows greater freedom of choice on how to implement them.

2.5.2 ISO/IEC 27002:2013 (Code of Practice for Information Security Management)

ISO/IEC 27002:2013 is the former ISO/IEC 27002:2005, which gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking

into consideration the organisation's information security risk environment(s). This standard is designed to be used by organisations that intend to:

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines.

According to Tipton and Krause (2011), the ISO/IEC 27002, is a standard that can be used as a basis for the development of security standards and security management practises within an organisation, and contains controls based on 11 areas such as information security policy, organising information security, information security incident management, access control and compliance, to name a few.

2.5.3 ISO/IEC 27003:2010 (Information technology - Security techniques - Information security management system implementation guidance)

ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It also describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

2.5.4 ISO/IEC 27004:2009 (Information technology - Security techniques - Information security management – Measurement)

ISO/IEC 27004:2009 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001. For example, an ISMS uses suitable metrics such as the percentage of personnel who annually received information security awareness training. Although this measure implies that ‘annual security awareness training’ is an acceptable approach, it does not measure learning or knowledge transfer, nor

does it measure the quality of awareness training sessions or its effectiveness. The current study aims to investigate the influence of awareness training on end-users' attitudes toward ISP compliance.

According to Nkwana (2015), government departments have a huge responsibility to ensure that they implement legislation that governs the protection of information security. Moreover, there is an emphasis that every organisation, regardless of the industry in which it operates, needs to comply with a number of external and governmental requirements related to information security practices and controls (Siponen and Willison, 2009; Susanto *et al*., 2012).

Basani (2012) further proposes that organisations should establish which legal, regulatory or statutory requirements they are subjected to in terms of their own business practices. Moreover, policies, standards and other security initiatives are needed to ensure regulatory compliance and enforceability (Basani, 2012). Likewise, Peltier (2014) suggests that when developing an information security policy, it will be necessary to establish a set of supporting standards. Thus the next section discusses information security initiatives adopted by the country in which this study was carried out.

2.6 INFORMATION SECURITY POLICIES INITIATIVES IN SOUTH AFRICA

South Africa (SA) has become aware of the significance of information security. This realisation lead to different initiatives being undertaken to address information security needs in the country. The initiatives undertaken included public–private partnerships, which have contributed positively in addressing information security threats and risks in SA (Basani, 2012).According to Whitman and Mattord (2011), organisations must implement a set of standards that clarify and define exactly what is inappropriate in terms of the rules of behaviour while working with organisational information. Moreover, Peltier (2016) suggest that when developing an information security policy, it is necessary to establish a set of supporting standards. In the exercise to develop and implement national policy of its executive authority, the Cabinet approved the Minimum Information Security Standards ("MISS") as the national information security document on 4 December 1996, made within the ambit of the National Strategic Intelligence act 39 of 1994 (Nkwana, 2015).

2.6.1 Minimum Information Security Standards (MISS)

The MISS is a standard that was drafted by the South African National Intelligence Agency (NIA) as an official government document intended to guide all government departments on information security. This standard was edited on March 1998 and should be maintained by all departments that handle classified information in the national interest of the country, to ensure that the national interests are protected subjected to the Public Service Act 103 of 1994 (MISS, 1998). However, the MISS is not a policy but a minimum standard that should be used as a guide when drawing up comprehensive security policy in dealing with various aspects of information security including applications, documents, communication and physical security measures of organs of the government (Basani, 2012; Nkwana, 2015).

According to Basani (2012), the MISS lays down minimum standards for handling classified information in all government institutions and the procedures and measures taken up in this document should be compiled to fit circumstances and operations of each of the institutions where classified information is handled. However, it is argued that this is not happening, as the implementation of “MISS” is not done fully in government departments (Nkwana, 2015). Consequently the Draft Information Security Policies was drafted.

2.6.2 Draft Information Security Policies (DISP)

According to the (DPSA article 159), the Department of Public Service and Administration (DPSA) has identified the need for a common policy on information security across the public service sector. Using the ISO/IEC 27001:2005 standard on information security; the DPSA developed the Public Service Information Security Policy aimed at ensuring the protection of government, business and citizens’ information in its custody by safeguarding its confidentiality, integrity and availability. Although the policy is still in its draft phase, it has been circulated widely for comment and review. Subsequently, the policy will be presented to Cabinet for approval.

This document presents a suite of integrated solutions, which together offer government organisations the tools necessary to integrate information security best practice into day-to-day business operations. Upon adoption this policy should serve

as a blue print for all organs of the state to abide by in implementing various categories of information security upon which a comprehensive information security culture may be built. According to the DPSA, ISPs are the cornerstone of information security effectiveness; without a policy upon which to base standards and procedures, decisions are likely to be inconsistent and security holes will be present, ready to be exploited by both internal and external persons. The DPSA ISP draft further postulates that the threat posed by the lack of consistency in IS initiatives by a nation can lead to unbearable consequences.

According to Basani (2012), policies and standards including security initiatives need to be communicated to the users, to ensure that users understand their security responsibilities, as well as how to act when faced with various security situations. Moreover, it is suggested that effective information security programs cannot be applied without implementing employee awareness and training programmes to address policy, procedures and tools (Peltier, 2016). Hence training and user awareness campaigns are proposed in literature. D'Arcy *et al*. (2009) suggests that organisations can use security education, training, and awareness (SETA) programmes to reduce users' information security misuse. Likewise, Ng *et al*. (2009) propose security awareness programmes for focusing on educating users about the possibility and damage of security threats and incidents so that users understand the need for security and their roles and responsibilities in protecting organisational information.

2.7 SUMMARY

According to Whitman and Mattord (2013), government organisations cannot protect the CIA of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. A wide enterprise awareness programme is therefore paramount to ensuring that people understand their IT responsibilities, organisational policies and how to properly use and protect the IT resources entrusted to them (NIST, 2003). Moreover the publication specifies that "it is expected that exposure to awareness activities will influence end-user behaviour and thus the security character of an organisation".

Chapter 3 : Information Security Learning

3.1 INTRODUCTION

This chapter presents the background of information security learning and its benefits for desired information security behaviour. A review of the background of information security learning is presented in Section 3.2. The chapter then concludes with a summary in Section 3.3.

3.2 INFORMATION SECURITY LEARNING BACKGROUND

In any literature on IS, it is impossible to avoid a discussion on the role of people in an IS program. It is well recognised that the greatest IS danger to any organisation is not a particular process, technology or equipment but rather the people who work within the "system" that hide the inherent danger (Tipton and Krause, 2011). Safa *et al*. (2015) suggest that users are an important threat to information security, in which careless intentional or negligent information security behaviour is the main problem. According to Merhi and Midha (2012) and Ghaffari, Sharifirad, Malekmakan and Hassanzadeh (2013), each employee should be taught and convinced to comply with information security rules and controls in order to successfully implement information security management. To achieve this, it is proposed that security education training and awareness (SETA) programmes are used as a means to influence employees' behaviour to comply with the information security policies. According to Bulgurcu *et al*. (2010), employees can be motivated to comply with ISPs by improving awareness through education that focuses on employees' beliefs and self-efficacy to apply the required security controls. Moreover, Puhakainen and Siponen (2010) suggest that the best way to ensure the feasibility of a security policy is to make sure employees are aware of the policy and understand it.

Likewise, the (NIST, 1998) propose three levels of learning in the learning continuum namely: awareness, training and education. According to the publication the awareness level is explicitly required for all employees as it sets the stage for training by changing organisational attitudes to realise the importance of security and the adverse consequences of its failure. The security basics and literacy level is a transitional stage between "awareness" and "training", which provides the foundation for subsequent training by providing a universal baseline of key security terms and

concepts and it is required for those employees who are involved in any way with IT systems. In today's environment this typically means all individuals within the organisation who are computer users. The education level on the other hand applies primarily to individuals who have made IT security their profession and focuses on developing the ability and vision to perform complex multi-disciplinary activities as well as the skills needed to further their IT security profession (NIST, 1998) Figure 3-1 below depicts the (NIST, 1998) learning continuum.

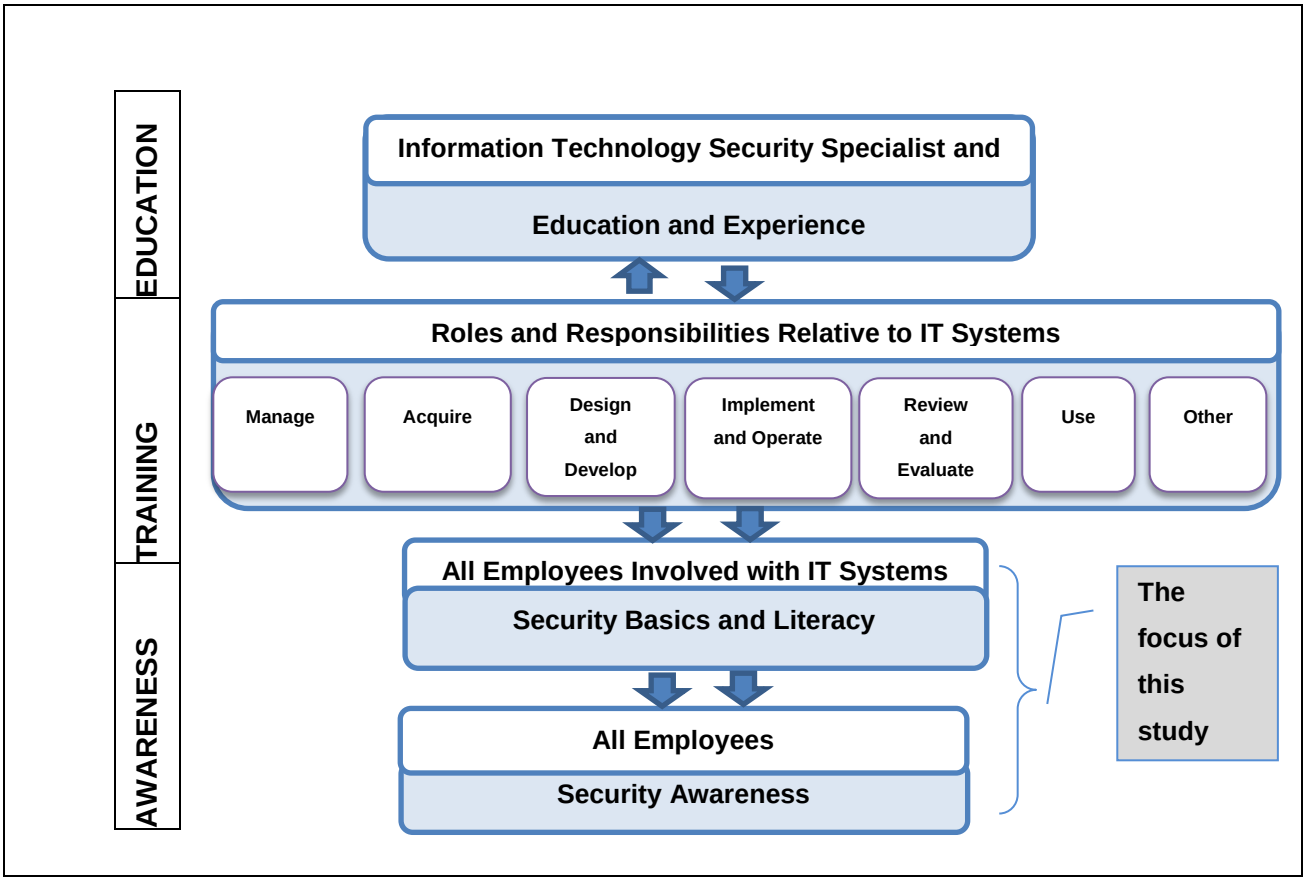


Figure 3-1: The (NIST, 1998) Learning Continuum

Ghaffari *et al*. (2013) indicate that information security awareness can lead to changes in behaviour, subsequently allowing people to be responsive to information security and thereby gradually changing the security culture of the organisation. A wide enterprise awareness programme is therefore paramount to ensuring that people understand their IT responsibilities, organisational policies and how to properly use and protect the IT resources entrusted to them (NIST, 2003). According to the (NIST, 2003) publication, this awareness programme should be focused on an organisation's entire user population.

Additionally, Ghaffari *et al*. (2013) state that increased security awareness on end-users can lead to increased security competence in complying with information security rules of the organisation. The following section therefore explains information security policy awareness.

3.2.1 ISP Awareness

According to Susanto and Almunawar (2012), information security awareness (ISA) is the stakeholder knowledge and attitude within an organisation to protect their physical and information assets. Furthermore, Bulgurcu *et al*. (2010) identify two types of awareness, the general awareness which is defined as an employee's overall knowledge and understanding of potential issues related to IS and their ramifications and the ISP awareness which is defined as an employee's knowledge and understanding of the requirements prescribed in the organisation's ISP and the aims of those requirements. The second definition of security awareness is adopted in this study.

The (NIST, 1998) indicates that awareness is a blended solution of activities to promote security, thus establishing accountability and informing the workforce of security news. Ghaffari *et al*. (2013) suggest that security awareness efforts are designed to reinforce good security practices and to change behaviour. Moreover, the purpose of awareness presentations is simply to focus attention on security, i.e. awareness presentations such as posters or video tapes are intended to allow individuals to recognize IT security concerns and respond accordingly (NIST, 1995). In addition the (NIST, 2003) indicates that an awareness programme is crucial in that it is the vehicle for disseminating information and a means to communicate IT security policies and procedures that need to be followed; thus users should first be informed of expectations. Ng *et al*. (2009) state that when users are aware of the likelihood of threats and effectiveness of security controls they can make a conscious decision to perform appropriate behaviour.

However, Khan, Alghathbar, Nabi and Khan (2011) indicate that it is generally understood by the IS professional community that user awareness represents a significant challenge in the security domain; for instance, users may be aware of a particular policy statement but might not know how to apply it, e.g. users might be aware that using passwords is a necessary precaution but may not know how to

change them whenever they comprised). (Bulgurcu *et al.*, 2010). Despite the importance of information security awareness, there seems to be a paucity of empirical studies that analyse the impact of information security awareness on IS behaviour. Authors such as Puhakainen and Siponen (2010) and Bulgurcu *et al*. (2010), have called for further research that demonstrates the value and the significant contribution of IS awareness efforts. Although other studies show that IS awareness can directly or indirectly alter employees' belief sets about compliance with the ISP, suggesting that creating a security-aware culture within the organisation will improve IS (Bulgurcu *et al.*, 2010; Merhi and Midha, 2012), it can also be established that an effective information security programme cannot be implemented just with ISP awareness without a training programme to address procedures on how to conform with the ISP. Thus the next section discusses and examines ISP awareness training.

3.2.2 ISP Awareness Training

According to (NIST, 1998), awareness is not training, the similarity between security awareness and security training is that they both seek to achieve sustainable attitudinal and behavioural improvements towards policies in end-users. Security awareness activities are methods to advertise IS through influential information-sharing techniques, whereas security training is learning through lessons which teach the skills and knowledge needed to comply with IS policies (Puhakainen, 2010). Similarly, Ng *et al*. (2009) state that security awareness programmes should train users on the purpose and functions of security controls, be it technical, physical or human controls, as this helps users to understand the benefits of controls and how they mitigate the risk of security threats.

Moreover, Whitman and Mattord (2011) suggest that national organisations cannot protect the confidentiality, integrity and availability (CIA) of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. Thus basic security and literacy training is used to explain the rules of behaviour for using the department's information systems and information, thereby establishing a level of expectation on the acceptable use of the information and information system (NIST, 1998). According to (NIST, 1998), basic security and

literacy training is the bridge between awareness and role-based training, which strives to build a foundation of information security terms and concepts in an organisation's information system user population upon which later role-based training, if required can be based. To draw an analogy with reading literacy, just as a child would learn to recognise and memorise letters of the alphabets and learns how to use them in principles of grammar and sentence structure to read and become literate, so too is security basics and literacy the foundation for further specific learning related to one's role(s) with respect to IS (NIST, 1998).

According to Ng *et al*. (2009), security training ensures that users are equipped with the confidence in their skill to practice the appropriate security behaviour, thus making employees believe that they are able to perform the recommended security. Furthermore, the (NIST, 1998) indicates that information security literacy refers to an individual's familiarity with and the ability to apply a core knowledge set, hence informing users of the threats and vulnerabilities that impact their organisation and personal work environments by explaining the "what" but not the how of security, and communicating what is and what is not allowed is suggested by the publication. Table 3-1 below represents the framework of the learning continuum adopted from the (NIST, 1995) to differentiate security education, training and awareness and what they represent. The focus of this study is highlighted.

Table 3-1: The (NIST, 2003) framework of of Security Education, Training and Awareness.

	Awareness	**Training**	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insights
Objective	Recognition	Skill	Understanding
Teaching method	Media • **Videos** • News Letters • Posters	Practical instruction • **Lecture** • Case study • Hands on practice	Theoretical instruction • Discussion seminar • Background reading
Test Measure	Identify learning	Apply learning	Interpretation of what was learned
Impact time frame	Short term	Intermediate	Long term

According to Whitman and Mattord (2011), one method of ensuring that policies are read and understood by general users is to provide training on those policies. These general users also require training on the technical details of how to do their jobs securely, including good security practices, password management and violation reporting (Ghaffari *et al*., 2013). Similarly, awareness training not only communicates ISPs and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for non-compliance (NIST, 1998). Hence the publication offers the following basic and literacy training (awareness training) objectives:

- To promote personal responsibility and positive behavioural change throughout an organisation's information and information systems user population beyond what is disseminated in the organisation's basic awareness efforts.
- To offer an information security awareness training curriculum framework to promote consistency across governance.
- To ensure that users of information and information systems understand the core set of key terms and essential information security concepts that are fundamental for the protection of information and information systems.

According to the (ISO/IEC 27002, 2013), all employees of the organisation and third party users should receive appropriate training and regular updates in organisational policies and procedures, including security requirements and legal responsibilities. Moreover, the (NIST, 2003) explains that security awareness programmes are designated to change behaviour and reinforce good security practices. The (NIST, 2009) specifies that awareness training programs must be structured in a way that changes both the perception and behaviour of an individual, thus increasing the likelihood that when a security event happens, the appropriate response will occur. Having examined what ISP awareness and training is, the following section discusses its benefits.

3.2.3 Benefits of ISP awareness training

Susanto and Almunawar (2012:2) state that: “The focus of information security awareness should be to achieve a long term shift in the attitude of employees towards security, whilst promoting a cultural and behavioural change within an organization”. Furthermore, Knapp and Ferrante (2012) suggest that IS managers should prioritise their effort largely on policy awareness, as it had the largest impact on effectiveness in their study. Merhi and Midha (2012) also suggest that security training has been shown to be an important factor impacting employees’ intentions to comply with an organisation’s ISPs.

According to Whitman and Mattord (2011), the purpose of awareness and training is to enhance security by improving awareness of the need to protect system resources and developing skills and knowledge so that computer users can perform their jobs more securely while using IT systems. Additionally, security awareness and training offer major benefits, as they improve employee behaviour by informing members of the organisation about where to report violations of policy and assist organisations to hold employees accountable for their actions (Merhi and Midha, 2012; Whitman and Mattord, 2011). Extant studies such as Herath and Rao (2009), Puhakainen and Siponen (2010), Merhi and Midha (2012) and Sommestad *et al*. (2014) have also highlighted the importance of IS awareness education and training. According to Ghaffari *et al*. (2013), many organisations have recognised the importance of implementing awareness training programmes for informing employees about information security and its related controls.

Moreover, Shaw (2012) has established that, in order for the programs to be successful, employees must reach acceptable levels in the three awareness dimensions that are discussed below:

- **Knowledge**

The first step for securing an organisation’s information is to acquire knowledge of security risks. Knowledge means identifying the presence of a threat and developing an awareness of it. The advantages of creating an accurate image of security threats can be enhanced by optimising observation and security awareness perceptions. Likewise Waly *et al*. (2012) suggest that providing employees with awareness and training programmes that describe the initial knowledge is the key to addressing all the security breach factors and the different types of vulnerability in the organisation.

- **Attitude**

To have enough knowledge about occurring security events and their impacts is not helpful in isolation. A positive attitude is needed for this knowledge to be used effectively. If users reach a sufficient level of perception regarding information security, it can prove beneficial to both them and the organisation. Moreover, Safa *et al*. (2015) suggest that human behaviour can change based on one's attitude.

- **Behaviour**

In this dimension, when employees develop good security behaviour, a strong information security culture within the organisation is established. The ultimate objective of an effective program of security awareness is making the users prepared to react to potential security risks.

3.3 SUMMARY

This chapter discussed information security education background, specifically the role of ISP awareness training and its benefits on ISP compliance. Although implementing an information security awareness program is crucial, it is necessary to measure how effective a particular method is in fulfilling its purpose (Khan *et al*., 2011). Moreover, Puhakainen and Siponen (2010) indicates that there is a need for IS training programmes that are based on theories to provide empirical explanations of how and why the programmes work. Thus the next chapter present the theoretical framework underpinning this study, in order to illustrate the influence of ISP awareness training on end-user’s attitudes toward compliance.

Chapter 4 : Theoretical Framework

4.1 INTRODUCTION

This chapter discusses the theoretical framework underpinning this study in Section 4.2. Section 4.3 discusses the role of attitudes in information security behaviour. The proposed research model is presented in Section 4.4 and the research objectives and hypotheses formulated are then discussed in Section 4.5 and 4.6 respectively. Section 4.7 provides the summary.

4.2 THEORETICAL FRAMEWORK

The theoretical foundation of this research is based on the Theory of Planned Behaviour (TPB), which is an extension of theory of reasoned action (Fishbein and Ajzen, 1975). According to the TPB, human action is influenced by three factors, namely: a favourable or unfavourable evaluation of the behaviour (attitude toward the behaviour); the perceived social pressure to perform or not to perform the behaviour (subjective norms); and the perceived capability to perform the behaviour (perceived behavioural control) (Ajzen, 2005; McEachan, Conner, Taylor and Lawton, 2011). Ajzen (2005) further states that these three antecedents lead to the formation of behavioural intention, as the more favourable the attitudes and social norms towards the behaviour and the greater the perceived behavioural control (PBC) and its outcome, the stronger the intention to enact the behaviour should be.

The theory is chosen as it is one of the most widely applied and successful theories to explain human behaviour (Tipton and Krause, 2011; Takemura, 2012). Moreover, recent studies on user's compliance behaviour towards ISPs have adapted the TPB to investigate information system's ethical behaviours and individuals' decisions to comply with ISPs (Bulgurcu *et al*., 2010; Ifinedo, 2012; Merhi and Midha, 2012; Humaidi and Balakrishnan, 2013a; Safa *et al*., 2015). Consistent with such previous studies, we posit that end-users' intentions to comply with an ISP will be influenced by attitude and perceived behavioural control (self-efficacy). Furthermore, Ajzen (1991) suggests that the TPB was developed to explain and predict human behaviour, thus intentions to perform behaviour can be predicted with high accuracy from attitudes toward the behaviour, additionally, these intentions together with the perceived behavioural control, account for considerable variance in actual behaviour.

According to Sentosa and Mat (2012), the TPB provides a robust theoretical basis for testing whether attitudes are indeed related to intend to engage in a particular behaviour. Moreover, Ajzen (2005) indicates that the behavioural belief (attitude) is the subjective probability that the behaviour will result in a certain outcome. Likewise, Safa *et al*. (2015) suggest that human behaviour can change based on one's attitude, which is a significant point as the behaviour component is the feedback mechanism for our attitudes. Hence this study investigates attitudes as targets of change to determine the influence ISP awareness training has on end-users' attitude toward ISP compliance. The following section thus discusses the role of attitudes in behavioural change.

4.3. THE ROLE OF ATTITUDES IN INFORMATION SECURITY BEHAVIOUR

According to Maio and Haddock (2010), attitudes are important as they influence how we view the world, what we think, and what we do. Azjen (1991) indicates that attitudes are informed by beliefs needed to engage in behaviour. Similarly, Tipton and Krause (2011) define attitudes as people's positive or negative response to something, for example if a user has a negative attitude towards privacy (confidentiality), they are more willing to share their username and passwords, which in turn will compromise the confidentiality of the information; whereas if they have a positive attitude toward a new corporate security program, they are more likely to abide by it as well as support it. Tipton and Krause (2011) suggest that attitudes not only define our feeling towards something, but also play a role in people's behaviour. Since attitudes are vital in understanding human thought and behaviour, social psychologists have devoted much attention to understanding how people form attitudes, how our attitudes influence our daily life, and how our attitudes change over time (Maio and Haddock, 2010). Early research also considered the degree to which individuals' attitudes influenced their behaviour. In the last thirty years, research findings have led to a more optimistic conclusion that attitudes do predict behaviour, in some conditions better than others (Maio and Haddock, 2010).

According to Tipton and Krause (2011), using psychological principles that social scientist and psychologist have discovered can aid in producing security awareness programmes that are more relevant and influential. Consequently information security professionals began an awareness campaign called the human firewall, which recognises that one of the major goals must be to change the attitudes and

behaviour of people involved in information security in accordance with the specific guidelines and policies that best fit their organisation (Tipton and Krause, 2011).

Because the human factor is ultimately an element that is exploited in a variety of attack scenarios (Khan *et al*., 2011), the people factor, and not technology, is key to providing an adequate and appropriate level of security (Knapp and Ferrante, 2012). However, as mentioned earlier, the human element is often seen as the weakest link in security (Rastogi and Von Solms, 2011). Thus if people are the key, but are also the weak link, more and better attention must be paid to people (Knapp and Ferrante, 2012). Moreover, Ng *et al*. (2009) indicate that employees in an organisation play an essential role in the prevention and detection of security incidents, and just as system administrators are responsible for configuring the technical controls, so are users responsible for practicing security counter measures such as choosing and protecting appropriate passwords.

However, Safa *et al*. (2015) argue that end-users' attitudes and their resistance behaviour change when they are faced with a mandatory password change, resulting in intentional password change delays because they consider it an unnecessary interruption.

Moreover, Maio and Haddock (2010) accentuate that policy makers are increasingly interested in discovering how to make attitudes exert a stronger effect on behaviours that people find difficult to enact. Likewise, Tipton and Krause (2011) propose attitudes as targets of change by suggesting that if you can subtly or directly change someone's attitude, you can consequently change their behaviour, as it is if often easier to change behaviour through an attitude shift than to change behaviour directly. For example, a repeated behaviour of leaving a workstation logged on while away is difficult to change directly as opposed to a strong emotional appeal toward an individual's attitudes about the impact it will have on the confidentiality of the information stored on that workstation, which might have a better effect. Therefore, the next section discusses the construct attitude.

4.3.1 Bases Of Attitudes

One popular conceptualisation of the attitude construct is based on Hovland and Rosenberg's (1960) tripartite model, which presents attitudes as the amalgamation of three separate measurable components: affect or feelings, cognitions or beliefs, and actions or behaviour. According to Tipton and Krause (2011), the affective

components are the emotional aspect of our attitudes, as our feelings towards an object play an important role in determining our attitudes (e.g. people are more likely to partake and do things that make them feel good). The cognitive component is the thinking aspect of our attitudes; opinions toward an object or subject can be developed based solely on insightfulness and process-based thinking.

The shared evaluative character of the cognitive and affective attitudinal components has sometimes been a source of confusion, due to people not always being aware of the bases of their attitudes. Sometimes people tend to believe that their attitudes are primarily based on cognition when they are in fact based on affect; nevertheless they both influence how people respond to persuasive messages (Moser *et al*. 2003; Ajzen, 2005). Furthermore, Moser, Uzzell, Millon and Lerner (2003) suggest that it is generally more effective to change attitudes that are actually based on emotion with emotional strategies than with more cognitively rational ones. Moreover, Tipton and Krause (2011) urge information security professionals to be aware of the structure and function of attitudes as they predict behaviour and are targets of change. Thus the following section discusses how attitude is formed.

4.3.2 Attitude formation

According to Hockenbury and Hockenbury (2007) there are a number of different factors that can influence how and why attitudes form, these factors are discussed the authors as follows:

Experience:

Attitudes form directly as a result of experience. They may emerge due to direct observation or personal experience.

Social Factors:

Social roles and social norms can have a strong influence on attitudes. Social roles relate to how people are expected to behave in a particular environment, thereby involve society's rules for what behaviours are considered appropriate.

Learning:

Attitudes can be learned in a variety of ways. Conditioning and observation learning are the two ways that can be used to alter attitude. This factor has been adopted in

this study to determine the influence it has on end-users'attitudes toward ISP compliance.

4.3.3 Attitude Change

The previous sections established a foundation for understanding what attitudes are and how they are constructed. This section expands on how attitudes can be influenced to motivate, predict, and even change behaviour. According to Tipton and Krause (2011), the specific influence of attitudes and behaviour is known as persuasion, because in order for a security awareness programme to be effective, people's attitude or mind-set towards change must be transformed.
Furthermore, Moser *et al*. (2003) and Spielberger (2004) suggest that the same factors that lead to attitude formation can also create attitude change as follows:

Learning Theory of Attitude Change: Classical and operant conditioning, as well as observational learning can be used to bring about attitude change. Classical conditioning can be used to create positive emotional reactions to an object by associating positive feelings with the target object, whilst operant conditioning can be used to strengthen desirable attitudes and weaken undesirable ones. Furthermore, people can also change their attitudes after observing the behaviour of others.
Elaboration Likelihood Theory of Attitude Change: This theory is also known as the theory of persuasion, which suggests that people can alter their attitudes if they are motivated to listen and think about the message, thus leading to an attitude shift, or they can be influenced by characteristics of the speaker, leading to a temporary shift in attitude. Moreover, messages that are interesting and stimulating are more likely to lead to permanent changes in attitudes.
Dissonance Theory of Attitude Change: Thus theory suggests people can also change their attitudes when they have conflicting beliefs about a topic. In order to reduce the tension created by these incompatible beliefs, people often shift their attitudes.

It can be inferred from the above discussion that there are various ways to change attitude. However, literature suggests that learning is the most important factor to alter/change attitude (Tipton and Krause, 2011; Merhi and Midha, 2012; Ifinedo, 2014). As indicated in Chapter 3, there are three levels of learning: awareness,

training and education. According to Knapp and Ferrante (2012), the goal of awareness and training programmes is to enhance knowledge of corporate policies and improve employee security behaviour in organisations. Moreover, the NIST, 2009) stipulates that the programmes must be structured in a way that changes both the perception and behaviour of an individual, thus increasing the likelihood that when a security event happens, the appropriate response will occur. Additionally, Dinev and Hu (2007) state that awareness represents a user's raised consciousness and understanding of security issues as well as strategies of how to deal with them. Since this study proposes a model based on the TPB to investigate the influence of ISP awareness training on end-users' attitudes toward compliance, the proposed research model and hypotheses are discussed.

4.4 THE PROPOSED RESEARCH MODEL

The objective of this study is to understand the antecedents of an employee's compliance with the ISP of their organisation by proposing and testing a model with the factors that influence an end-users' attitudes and in turn their intention to comply with their organisation's Information Security Policy (ISP). This model is based on the Theory of the Planned Behaviour (TPB) as discussed in the previous section. It is suggested that the intention to perform various kinds of behaviours can be predicted with high accuracy from attitudes toward the behaviour, subjective norms, and perceived behavioural control. While attitudes toward the behaviour and social norm are expected to influence intend, it is the perceived behavioural control that is seen as decisive for action, e.g. if a person does not perceive to have control over the behaviour and its outcomes the intention to perform that behaviour is unlikely, even if the person has a positive attitude toward the behaviour *(*Azjen, 1991), hence it is postulated that intentions, together with PBC, account for considerable variance in actual behaviour*.*

According to Herath and Rao (2009), Bulgurcu *et al*. (2010) and Al-Omari *et al*. (2013), attitude as a mediator and its antecedents (behavioural beliefs), can be reshaped by external interventions. For this reason this study expand on the TPB by adding external interventions (i.e. ISP awareness training) to reshape end-users' attitudes to determine the influence of these interventions on their intentions to comply with their organisation's ISP.

However, since Ajzen (2005) suggests that not all TPB constructs need to be significant to successfully explain intentions, as the relative importance of the three constructs is likely to change, this study excluded subjective norms in the proposed research model. The rationale being that subjective norms in other studies like Sheraan (2002), McEachan *et al*. (2011) and Sentosa and Mat (2012) have been found to produce low meta-analysis when used with the other TPB constructs. Likewise, a weakness in the subjective norms-intention association, in comparison with attitude-intention and perceived behavioural control-intention associations has been identified (Armitage and Conner, 2001). According to Topa and Moriano (2010), the lack of association of subjective norms-intention indicates that intentions are influenced primarily by personal factors, i.e. attitudes and perceived behavioural control.

Hence this study adopts the attitudes and perceived behavioural control constructs from the TPB, to determine the influence of an external intervention (ISP awareness training) on end-users' attitudes toward complying with their organisation's ISP. Moreover, McEachan *et al*. (2011) postulates that individuals subjected to an intervention are exposed to new information that may well change some of their behaviour-relevant beliefs, and as a result affect their intentions and behaviour. Therefore, Figure 4-1 depicts the proposed research model for this study. H1-H5 are the research hypotheses, which are discussed in section 4.6.

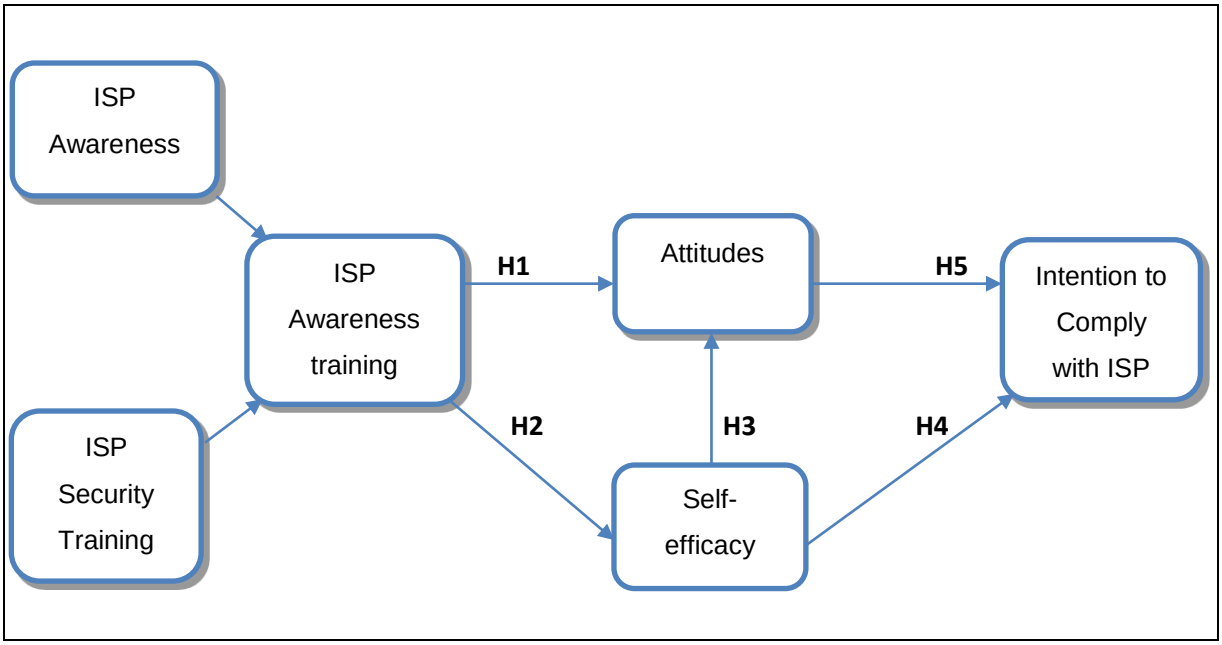


Figure 4-1: The Proposed ISP Compliance Model

4.4.1 External Interventions

Ajzen (2002) recommends including external interventions to the TPB model to investigate its ability to predict human behaviour, thus building on the TPB, ISP awareness and training approaches will be incorporated as an antecedent to the proposed model to determine an understanding of the influence of ISP awareness training on end-users' attitude towards ISP compliance. According to Puhakainen and Siponen (2010), all approaches (e.g. awareness and training) affecting end-user behaviour should satisfy the requirements of behavioural theories in order to be effective. Thus, this study will not only demonstrate the influence of ISP awareness training but will also contribute to its practical effectiveness on end-user attitudes toward complying with their organisation's ISP.

4.4.2 Constructs

As mentioned earlier in the chapter, only three constructs are adopted from the TPB in this study, namely: *attitude, perceived behavioural control* and *behavioural intention*. The *attitude* construct is defined as learned predisposition to respond in a consistently favourable or unfavourable manner with respect to the given object (Fishbein and Ajzen, 1975), while Ifinedo (2014) defines perceived behavioural control as the individual's beliefs regarding the efficacy and resources needed to facilitate behaviour. Other authors refer to the *perceived behavioural control* construct as people's perceptions of their ability to perform a given behaviour (Sentosa and Mat, 2012). According to Siponen et al. (2010), the perceived behavioural control is best taken care of by technical education (e.g. increases in skill/ability), which is hoped will make adherence to security guidelines very easy. Furthermore, Armitage and Conner (2001) present three types of perceived behavioural control measures, namely: Self-efficacy, perceived control and perceived behavioural control, where self-efficacy is defined as the confidence in one's own ability to carry out a particular behaviour and perceived control is defined as perceived controllability of a given behaviour; whilst perceived behavioural control is defined as the perceived ease or difficulty of performing a given behaviour (Ajzen, 1991).

According to Ajzen (2005), control beliefs underlie perceptions of behavioural control. Likewise, McEachan *et al*. (2011) indicate that the perceived behavioural

control is based on salient control beliefs. These beliefs are concerned with the presence of factors such as required skills, abilities, availability/lack of time, and can furthermore facilitate or inhibit performance of behaviour (Ajzen, 1991; McEachan *et al*., 2011), e.g. if users do not have easy access to the policies, or they do not get support on how to comply with security policies, they are unlikely to comply with the policies. Furthermore, McEachan *et al*. (2011) suggest that control beliefs contribute to a sense of self-efficacy, in direct proportion to the factor's perceived power to facilitate or impede performance of the behaviour. Moreover, the perceived behavioural control is compared to Bandura's (1977) concept of perceived self-efficacy, thus, in the context of this study, an end-user's judgment of personal skills and knowledge about fulfilling the requirements of the ISP. Likewise, Warkentin, Johnston and Shropshire (2011) suggest that self–efficacy refers to the degree to which an individual believes in their ability to enact the recommended reaction. Therefore, in this study self-efficacy is adopted instead of perceived behavioural control, as the perceived behavioural control measures the same latent construct as self-efficacy (Fishbein, 2005; Ajzen, 2011).

However, some studies suggest that perceived behavioural control and self-efficacy are not synonymous (Ajzen, 2002; Dishman, Motl, Saunders, Felton, Ward, Dowda and Pate. 2005). According to Ajzen and Timko (1986), self-efficacy focuses on factors internal to the individual, whereas perceived behavioural control reflects external and internal factors. Furthermore, Ajzen (1991) suggests that internal factors include beliefs about skills, abilities, and self-control, whereas external factors include time and opportunity. In the current study the use of self-efficacy is consistent with the existing literature (i.e. Pahnila *et al*., 2007; Herath and Rao, 2009; Bulgurcu *et al*., 2010; Ifinedo 2012 and 2014; Kim *et al*., 2014; Siponen *et al*., 2014). These studies signified the relevance of self-efficacy to ISP intention to comply behaviour.

Having discussed the research constructs in this study, the following section discusses the research objectives and formulates the hypotheses.

4.5 RESEARCH OBJECTIVES

This section reiterates on the purpose of this study. The first objective of this research is to determine end-users' level of ISP awareness training and current

compliance behaviour in order to make inferences about their existing knowledge regarding the information security policy of their organisation and thus the organisation's information security culture. The first research question is:

- *What is the current level of end-users' ISP awareness training and compliance behaviour?*

The second research objective is to empirically validate the proposed research model, to assess the influence ISP awareness training has on end-users' attitudes toward ISP compliance, thus the following research question was formulated.

- *How does ISP awareness training influence end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP?*

To answer this research question, the related hypotheses (H1-H5) as indicated in Figure 4-1 are discussed in the next section.

4.6 RESEARCH HYPOTHESES

As mentioned earlier, attitudes are people's positive or negative response to something, for example if a user has a negative attitude towards privacy (confidentiality), they are more willing to share their username and passwords, whereas if they have a positive attitude toward a new corporate security program, they are more likely to abide by it as well as support it (Tipton and Krause, 2011). Moreover, one of the most effective ways of producing change in human behavioural beliefs (attitudes) is said to be persuasive communication (Tipton and Krause, 2011). Likewise, the (NIST,2003) stipulates that one of the factors that influence user security behaviour is what they are told, and in most organisations this takes the form of security awareness initiatives. In the context of this study, ISP awareness training is implemented as an antecedent of end-users' attitudes toward complying with their organisation's ISP. Moreover, Mattord and Whitman (2008) indicate that the purpose of awareness training is to enhance security by improving consciousness of the need to protect system resources and to develop skills and knowledge. Therefore the following hypothesis is posed:

H1 -> ISP Awareness training directly affects an end-users' attitude to comply with their organisation's ISP.

According to Ifinedo (2014), self-efficacy relates to an individual's abilities to cope with a given behaviour. It is further postulated that individuals with high IS capabilities realise the importance of following organisational ISP, as they are able to better understand the dangers of non-compliance (Ifinedo, 2014). Likewise, Pahnila *et al.* (2007) emphasise that if users lack appropriate skill/ability and do not have easy access to policies nor do they get support on how to comply with security policies, they are unlikely to comply with the ISPs. Moreover, Humaidi and Balakrishnan (2013b) suggest that awareness and training should be provided to increase users' skill and understanding towards complying with ISPs. According to Warkentin *et al*. (2011), the confidence in one's own ability to carry out a particular behaviour is facilitated by self-efficacy. Therefore the following hypothesis is deposited:

H2 -> ISP Awareness training positively affects an end-users' self-efficacy to comply with their organisation's ISP.

Self-efficacy, which refers to individuals' belief in their own competence and capabilities (Bandura, 1977), is indicated to highlight the extent to which individuals either pessimistically or optimistically feel and think about motivating themselves to completing specific tasks or actions (Ifinedo, 2014). Furthermore, based on the TPB, an end-user's beliefs about a given behaviour will influence their attitude toward that behaviour (Ajzen 1991). In the context of this study an end-user's beliefs (self-efficacy) about fulfilling the requirements of the ISP will influence their attitude towards complying with the ISP. Thus we hypothesis that:

H3-> Self-efficacy has a positive influence on end-users' attitudes toward complying with their organisation's ISP.

Compeau and Higgins (1995) indicated that people with higher levels of self-efficacy will employ a given task or behaviour more than those with low self-efficacy. With respect to ISP, Ifinedo (2012 and 2014) suggests that individuals with high IS capabilities will appreciate the need to follow organisational ISPs. According to Siponen *et al*. (2014), self-efficacy is the most powerful predictor of intention to comply with behaviour, and refers to an end-user's belief that he/she can apply and adhere to the ISP in the context of this study. Hence it is deposited that:

H4 -> Self Efficacy has a positive impact on end-users' intention to comply with their organisation's ISP

As previously indicated, Tipton and Krause (2011) propose attitudes as targets of change and suggest that it is often easier to change behaviour through an attitude shift than to change behaviour directly. Based on the existing literature about the TPB, it can be deduced that end-users' intentions to comply with the requirements of the ISP are associated with their attitudes towards compliance. Hence the following hypothesis is derived:

H5 ->The end-users' attitude towards complying with their organisation's ISP has a positive impact on their intention to comply.

4.7 SUMMARY

In this chapter the theoretical framework that forms the basis for this study was discussed and hypotheses were formulated. A research model was then proposed to assess ISP awareness training influence on end-users' attitudes toward compliance. The next chapter presents the research methodology and explains the research design and the different methods used to examine the proposed research model.

Chapter 5 : Research Methodology

5.1 INTRODUCTION

This chapter presents the overview of the research methodology in terms of the research approach, design and research methods applied in this study. The chapter commences with the discussion of the research foundation underpinning this study in Section 5.2. A discussion on Creswell's philosophical worldviews and the worldview of the present research then follows in Section 5.3. Thereafter, different research designs and the research approaches they are associated with are outlined in Section 5.4. Section 5.5 then discusses the research designs adopted in this study. Furthermore, the research methods in terms of population and sampling are outlined in Section 5.6, whilst data collection methods, reliability and validity of the research instrument are discussed in the subsequent chapter. Finally the ethical considerations are presented in Section 5.7 and Section 5.8 summarises the chapter.

5.2 RESEARCH FOUNDATION OF THIS STUDY

Figure 5-1 is based on Creswell's (2014) framework for research, which depicts the research methodology followed in this study. The areas highlighted in red indicate the specific research methodology followed for this study.

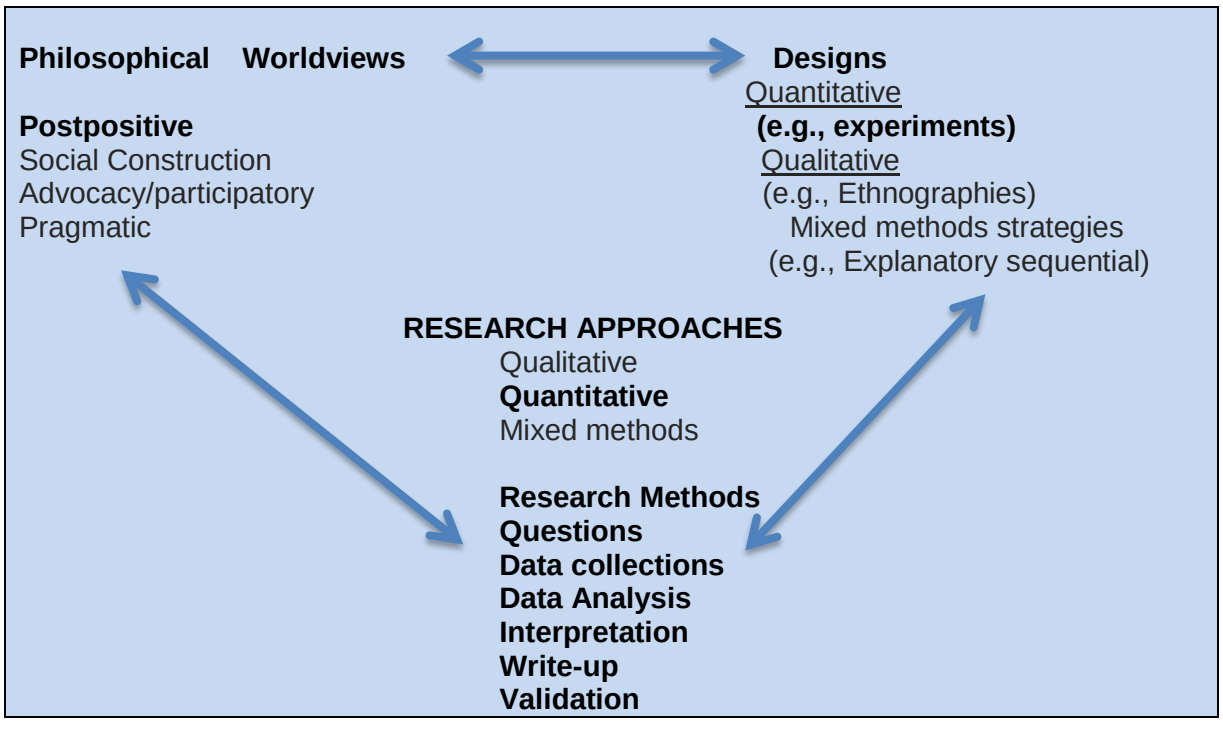


Figure 5-1: Creswell's (2014:5) Framework for Research

5.3 PHILOSOPHICAL WORLDVIEWS

According to Creswell (2014), the word worldview means “a basic set of beliefs that guide action”, which is also known as paradigms (Oates, 2006; Babbie, 2014). Worldviews are a general orientation about the world and the nature of research that a researcher holds (Creswell, 2014). Likewise, Oates (2006) indicates that a paradigm is a set of shared assumptions about some aspect of the world that is concerned with different communities’ shared way of thinking about how to do research and gain or create knowledge. This shared way of thinking is reflected in the research strategies used and accepted as appropriate in a particular research community (Oates, 2006). Creswell (2014) proposes four different worldviews (paradigms), namely: post-positivism, constructivism, transformative and pragmatism. Oates (2006) proposes three philosophical paradigms, namely positivism, interpretivism and critical research; whereas Welman *et al.* (2005) suggest two paradigms, positivism and anti-positivism.

According to Creswell (2014), the post-positivist assumptions are sometimes called positivist research, empirical science and post-positivism, henceforth positivism. The last term is called post-positivism because it represent the thinking after positivism, challenging the traditional notion of the absolute truth of knowledge and recognising that we cannot be positive about our claims of knowledge when studying the behaviour and actions of humans (Creswell, 2014). Creswell (2014) further indicates that the knowledge that develops through a positivist lens is based on careful observation and measurement of the objective reality that exists, thereby developing numeric measures of observations to study the behaviour of individuals. Likewise, Welman *et al*. (2005) suggests that positivists define their approach as the study of observable human behaviour and aim to uncover general laws of relationships and causality that applies to all people at all times.

The other different worldviews, such as constructivism or social constructivism, rely as much as possible on the participants’ views of the situation being studied, i.e. social constructivists believe that individuals develop subjective meanings related to their experiences. These meanings are numerous and diverse, leading the researcher to look for complexity of views rather than narrowing meanings (Creswell, 2014). Likewise, Oates (2006) suggests an interpretive study that does not prove or

disprove a hypothesis as in positivist research, but tries to identify, explore and explain how all the factors in a particular social setting are related and interdependent (i.e. interpretivists look at how people perceive their world and try to understand phenomena through the meanings and values that the people assigned to them). Additionally, Welman *et al*. (2005) indicate that anti-positivists are concerned with understanding human behaviour from the perspectives of the people involved.

Creswell (2014) indicates that other groups of researchers hold philosophical assumptions which can be described as transformative, which holds that the research enquiry needs to be intertwined with politics and political agenda, thus the research contains an action agenda for reform that might change the life of the participants, researcher or institutions in which individuals lives. Correspondingly, Oates (2006) proposes a critical research paradigm which asserts, similar to the view of interpretive researchers, that reality is created and re-created by people. The last worldview proposed by Creswell (2014) is pragmatism, which arises out of actions, situations and consequences rather than antecedent conditions as in positivism.

It is suggested that positivism assumes a deterministic philosophy in which causes probably determine effect or outcomes, and an outcome is defined as a means of testing objective theories by examining the relationship among variables (Creswell, 2014). Welman *et al.* (2005) also link positivism to a scientific model or an approach that strives to formulate laws applicable to populations. These said laws explain the causes of observable and measurable behaviour.

Since this study uses the theory of planned behaviour to assess the relationship of ISP awareness training and end-user attitudes towards complying with their organisation's ISP, the positivism worldview is seen fit to guide the suppositions of this study. The rationale is that positivism assumptions are more associated with quantitative research than qualitative research, as the problems studied by positivists reflect the need to identify and assess the causes that influence the outcomes. Having identified the philosophical worldview to which this study is underpinned, the next section explains the research design in terms of research approach.

5. 4 RESEARCH DESIGNS

The next element in the research framework used by Creswell (2014) is the research design that provides specific direction for the procedures that are included in a research approach. According to Hofstee (2006), a research design includes a discussion of the techniques used to answer the research questions. Likewise Creswell (2014) suggests that a research approach involves philosophical assumptions and distinct methods or procedures. Therefore the following section discusses the decisions informing the selection of a research design.

5.4.1 Dimensions of research approaches

According to Babbie and Mouton (2010), research can be categorised as follows:

- **Descriptive research:** is conducted in order to describe the precise measurements and reporting of the characteristics, features of the population or phenomenon under study. According to Babbie (2014), this research approach is one that provides a picture of the problem as it naturally occurs in its environment.
- **Explanatory research:** is described as research that seeks to identify causes, to ascertain causality between factors and to determine effects on behaviour of a social phenomenon; as well as to predict how one phenomenon will change or vary in relation to another variable (Pierson and Thomas, 2010). Moreover explanatory research focuses on analysing causal relationships (Babbie and Mouton, 2010).
- **Exploratory research:** is undertaken to develop an initial understanding of the phenomenon being studied. According to Babbie and Mouton (2010), exploratory research is conducted to gain new insights, discover new ideas and increase knowledge of a phenomenon

In this study a descriptive and explanatory research was adopted in order to determine the end-users' level of ISP awareness training and their current compliance behaviour. The rationale being that descriptive research is the kind of research that attempts to describe reality accurately as it exists naturally, so that an overview of the current status of a situation is obtained (Mertens, 2009 and Monette, Sullivan and Dejong, 2011). Furthermore, Salkind (2012) suggests that descriptive

research presents a picture of the specific details of a situation. In addition to the descriptive research adopted in the study, an explanatory study was also undertaken to assess the influence of ISP awareness training intervention on end-users' attitude toward ISP compliance. According to Babbie and Mouton (2010), an explanatory research is normally experimental in nature, where hypotheses can be tested by comparing groups. Thus a causal connection between the independent and dependent variable can be established in explanatory research (Babbie and Mouton, 2010). Furthermore, Ginsberg (2001) suggest that an explanatory research can be useful in programme evaluation in order to make statements about the influence of the programme on participants, as it focuses on causal relationships between the independent variable (the intervention) and the dependent variable (change in the behaviour) which is in line with the objective of the current study. Depending on the research conducted, research approaches and their underlining designs can be distinguished (Welman *et al.*, 2005 and Creswell, 2014).

5.4.2 Research Approaches and Associated Research Designs

According to Creswell (2014), certain type of social research problems calls for specific research approaches. Furthermore, Creswell (2014; 12) states that: "the researcher not only selects a qualitative, quantitative and mixed approach study to conduct a study; the enquirer also decides on the type of research designs within these three choices". The following section thus discusses the research approaches and the research designs they are associated with.

Qualitative Approach

Qualitative research is a means for exploring and understanding the meaning individuals ascribe to in a social or human problem, and is based on flexible and explorative methods enabling the researcher to change the data progressively, so that a deeper understanding of what is being investigated can be achieved (Creswell, 2014). According to Kumar (2014), a study is classified as qualitative if the purpose of the study is primarily to describe a situation, phenomenon, problem or event, and the information is gathered and analysed to establish the variation in the situation, phenomenon or problem without quantifying it. The following types of research designs are associated with a qualitative approach (Creswell, 2014):

- An **Ethnographic** design is a design in which a researcher studies a cultural group in their natural setting over a prolonged period by collecting primary, observational and interview data. Welman *et al*. (2005) explains that the primary task of ethnographic research is to uncover and explicate the ways in which people in a particular setting come to understand, account for, take action and manage the situations they encounter.
- **Grounded Theory** in this design the researcher derives a general abstract theory of a process, action or interaction grounded in the view of participants, i.e. the process involves the use of multiple stages of data collection, refinement and interrelationship of categories of information.
- **A Case study** allows a researcher to explore in depth a programme, event, activity, process and/or one or more individuals. Welman *et al*. (2005) elaborates that in a case study, a researcher is directed towards understanding the uniqueness and idiosyncrasy of a particular case in all its complexity.
- **Phenomenological research** allows a researcher to understand the lived experiences of participants and involves studying a small number of subjects through a prolonged extensive engagement to develop patterns and relationships of meanings.
- **Narrative research** allows a researcher to study the lives of individuals by asking one or more individuals to tell stories about their lives; these stories are then retold or narrated chronologically by the researcher.

The following scenarios are illustrated by Creswell (2014) to indicate how a qualitative approach combines into a research design:

A qualitative approach is said to assume a constructivist worldview and ethnographic design, where data is collected by means of observing participants' behaviour during their engagement in activities; or a transformative worldview and narrative design, where data is collected in the form of interviews to determine how participants have personally experienced a phenomenon or oppression. Thus, if a concept or phenomenon needs to be explored and understood, it merits a qualitative approach.

Quantitative Approach

Parahoo (2014) indicates that a quantitative approach arises from believing that human phenomena and variables in human behaviour can be studied empirically. According to Creswell (2014) a quantitative approach combines into a research design by undertaking a post-positivist worldview and an experimental design, where data is collected in an instrument that measures attitudes for instance, and the information is analysed using statistical procedures and hypothesis testing. Furthermore, Kumar and Phrommathed (2005) suggest that quantitative studies can also provide details of behavioural attitudes which are often based on surveys to help generalise the findings. However there are different types of research designs that are associated with a quantitative approach. Creswell, 2014 and Welman et al., 2005 explains them as follows:

- **Descriptive research design (surveys)** seeks to describe the current status of an identified variable.
- In a **Causal comparative research design,** a researcher compares two or more groups in terms of a cause that has already happened.
- **Correlational research design** is when a researcher uses a correlational statistic to describe and measure the degree of association between two or more variables.
- A **true experimental design** seeks to whether a specific treatment influences an outcome. This is assessed by providing treatment to one group and withholding it from the other and then determining how both groups scored on an outcome.
- In a **single-subject experimental design,** a researcher studies a single group and provides an intervention during the experiment, however there is no control group to compare with the experimental group.
- The **quasi-experiment design** uses a control and experiment group but participants are not randomly assigned to groups.

Since the current study aims to determine the level of ISP awareness training and the compliance behaviour of end-users, as well as to assess a model to investigate the influence of ISP awareness training on end-users' attitudes toward ISP compliance, the quantitative approach is deemed suitable to obtain the objective of

this study. The selection of the research design applied in this study is discussed later in the chapter.

Mixed Methods Approach

The mixed method approach on the other hand is only useful when a pragmatic worldview and both the qualitative and quantitative research designs are assumed due to qualitative or quantitative approach being independently inadequate to best understand a research problem Creswell (2014); In this scenario, Creswell (2014) suggests that a researcher will for instance begin with a quantitative design (e.g. a survey) in order to generalise the findings to a population and then apply a qualitative design (e.g. open-ended interviews) to collect detailed views from participants to help explain the initial quantitative survey. This is not the case in the current study as both quantitative designs (a survey and experimental designs) are applied. The selection for adopted designs is discussed in the next section.

5.5 SELECTED RESEARCH DESIGNS

According to Creswell (2014), the research designs associated with quantitative research are invoked by positivist worldview and include experiments and surveys. Moreover, it is suggested that positivists hold a deterministic philosophy in which causes probably determine effects or outcomes such as in experiments (Creswell, 2014). Likewise, Oates (2006) indicates that the positivism paradigm underlies the scientific method which mainly uses experiments as a way of collecting data.

In the present study, the researcher considered the most suitable research design to be a descriptive survey design and a true experimental design. According to Creswell (2014), the term survey can be used to designate any research activity in which the investigator gathers data from a portion of a population for the purpose of examining the characteristics, attitudes or opinions of that population. Unlike correlational design that tend to measure the degree of association between two or more variables using statistical data, and causal comparative research design which compares two or more groups in terms of a cause that has already happened (Creswell, 2014). A survey is chosen since one of the objectives in this study was to determine the end-users' level of ISP awareness training and their current ISP compliance behaviour; so that inferences can be made about their information security culture. Moreover the use of the survey provides an advantage of obtaining

characteristics and or behaviour of a large number of people all at once (Babbie, 2014). However, a key weakness in surveys is that, it is very difficult to realise insights relating to the causes of the behaviours involved in the phenomena measured (Welman *et al.,* 2005). According to Oates (2006), other research designs such as experiments can be used when surveys are not sufficient; Hence this study also undertakes an experimental design, to assess the influence ISP awareness training has on end-users' attitudes towards ISP compliance.

The type of experimental design that this study undertakes is a true experimental design. Since, single-subject experimental designs have no control group to compare with the experimental group and quasi-experimental designs have no random assignment of participants to different groups, resulting in groups that may differ from one another in terms of nuisance variables as well as the independent variable (Welman *et al*., 2005). According to (Welman *et al*., 2005 and Leary, 2012), a true experimental design follows a procedure where participants are randomly assigned to groups, in order to eliminate the possibility of systematic differences (bias) among participants that could affect the outcome, so that any difference in the outcome can be attributed to the experimental treatment.

Figure 5-2 depicts the research designs applied in this study and how they correlate

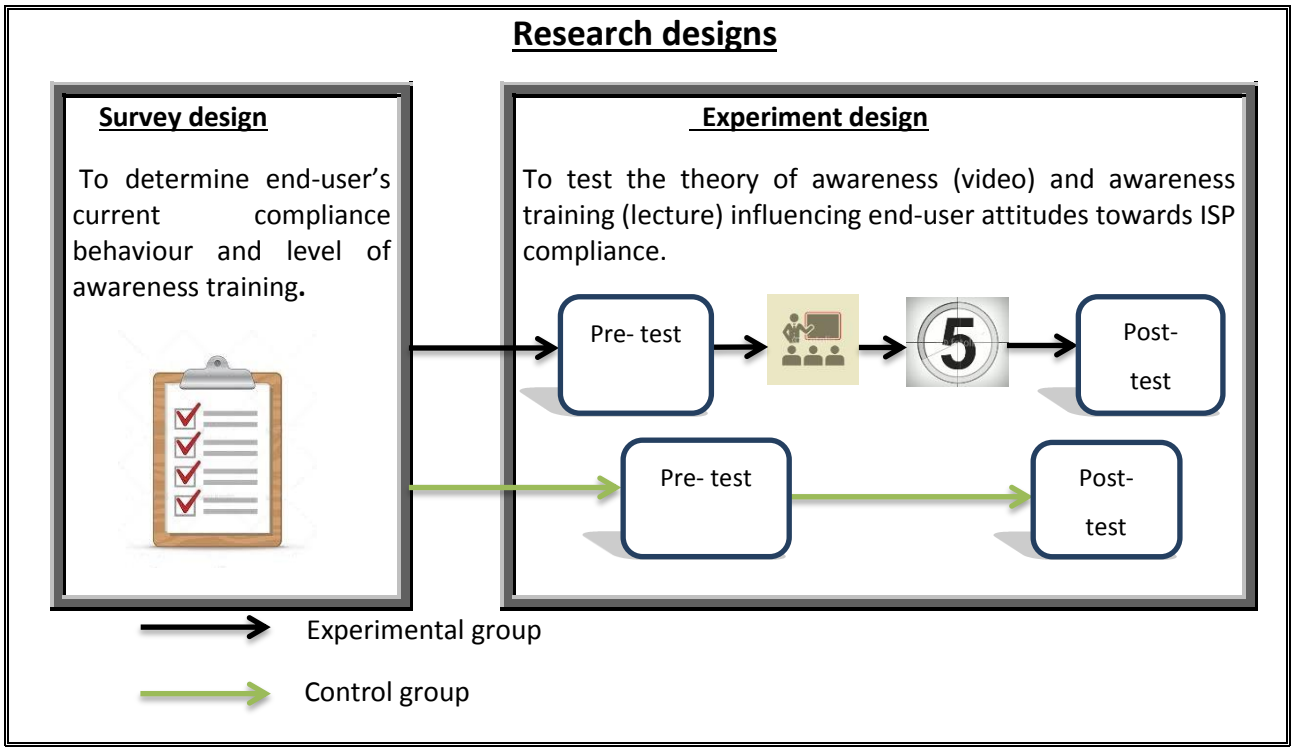


Figure 5-2: Diagrammatic presentation of the research design

The next section discusses the research methods used to collect data in this study.

5.6 RESEARCH METHODS

According to Creswell (2014), the third major element in the design framework is the specific research methods, such as data collection, analysis and interpretation. The procedure for these research methods are discussed in Chapter 6. Furthermore, when conducting a study, data is collected from subjects of enquiry. Therefore the following section defines the population and sample from which data was collected.

5.6.1 Population and Sample

Stangor (2011) indicates that the entire group that the researcher desires to learn about is known as the population, and the smaller group of people who actually participate in the research is known as the sample. According to Stangor (2011), sampling refers to the selection of people to participate in a research project, usually with the goal of being able to use these people to make inferences about a larger group of individuals. In this research permission to conduct the study was granted by a government organisation located in the North West province, the organisation consists of three distinct strata with different sizes, functions and culture.

5.6.2 Sampling Procedure

There are many different methods of sampling and these can be categorised into non-probability and probability sampling techniques. According to Babbie (2014), the idea behind probability sampling is to have a sample of individuals that contain the same variations existing in the population, in order to provide useful descriptions of the total population. Furthermore, Welman *et al*. (2005) suggest that generalisation about populations from data collected using any probability sample is based on probability, thus the larger the sample size the lower the likely error in generalising. By relying on a random process for the selection of participants, Babbie (2014) indicates that the possibility of bias in the selection procedure is largely eliminated and the chances of generating a representative sample is enhanced. On the other hand, non-probability sampling is a technique in which units of the sampling are chosen based on convenience (Welman *et al*., 2005; Babbie, 2014).

However, the organisation in which the study was conducted granted permission to conduct the study on condition that a list of computer users is not provided for the research to assure anonymity. Therefore, two levels of sampling were carried out.

Firstly, a communiqué by the organisation was made to all end-users in the province, informing them about the dates on which the research will be conducted on for different locations, what the research entails and the duration. Consequently, a convenience sample was obtained. Although a probability sampling technique would have been preferred, the convenience sample was the only sampling technique that could be used to collect the data. Irrespective of the non-representativeness of convenience sampling, Oates (2006) suggests that if research is concerned, for example with students' views, the survey respondents should be students. However if the research is about some aspect of computer system in the world beyond a university, using students because they were convenient would be criticised (Oates, 2006). In this context, this study is concerned with end users of a government organisation, thus the participants were end users of a government organisation. Furthermore, Welman *et al.* (2005) accentuate that although the likelihood of the sample being representative is low in convenience sampling, this problem is less important where there is little variation in the population and the sample.

Secondly, from the convenient sample obtained, end-users were then randomly assigned to two equal groups (the experimental and control group). Each participant was given a unique numbered tag ranging from 1 to *n* for identification. The odd numbered participants were the control group whereas the even numbered participants were the experimental group. According to Welman *et al*. (2005), this procedure eliminates the possibility of systematic differences among characteristics of the participants that could affect the outcomes, so that any differences in outcomes can be attributed to the experimental treatment. Furthermore, Leary (2012) states that only when a two group random assignment experimental design is applied can it be determined whether the different levels of the independent variable led to differences in participants' behaviour. Moreover, Trochin (2006) suggests that random selection is how a sample of people is drawn for a study from a population, whilst random assignment is how a sample that was drawn is assigned to different

groups or treatments in a study. Furthermore, it is possible to have either a random selection or random assignment (Trochin, 2006) in a study.

The total number of unique tags handed out was 221 with the sample size dispersed per stratum as shown in Table 5-1 below.

Table 5-1: Sampling Summary

Strata	Sample size	Valid Responses
Mafikeng	57	38
Potchefstroom	142	119
Zeerust	22	16
Total	**221**	**173**

A total number of 221 end-users participated in the study; however only 173 responses were found to be valid for analysis, due to incomplete responses. Thus the final, viable sample size for this study is 173.

5.6.3 Sample size

According to Burns and Bush (2010), the sampling size has an effect on how the findings accurately represent the population from which the sample was drawn; as the larger the sample, the more likely it is that the generalisation is an accurate reflection of the population (Saunders, Lewis and Thornhill, 2009). However, Hair Jr, Black, Babin and Anderson (2014) and Welman *et al.* (2005) suggest that by involving specified inclusion criteria, the sample becomes homogeneous, which means that there is not much difference between the sample and the population, thereby permitting a smaller sample size.

Additionally Hair *et al*. (2014) suggest that the sample size depend on factors such as time and money to collect the data. Furthermore sample size also depends on statistical analysis used in a study (Sauders *et al*., 2009). For many statistical procedures such as t-tests, the central limit theorem can be applied (Levine, Szabat and Stephan, 2016). However, Pearson and Mundfrom (2010) argue that the issue with the sampling size for Exploratory Factor Analysis (EFA) is not as straight forward due to subjectivity. According to Pearson and Mundfrom (2010), the statistical problem with EFA is the estimation of

communalities and factor loadings. Although EFA sampling size is a challenge there are several guidelines in literature.

The two categories of guidelines in terms of minimum sample size in factor analysis are the absolute or least number of cases (N), and the subject-to-variable ratio (p).

A summary of guidelines for the least number of cases are presented as follows:

Rule of 100: MacCallum *et al*. (1999) recommend a sample of at least 100 cases. Likewise, Hair *et al*. (2014) suggest that a sample size of at least 100 cases is needed for factor analysis.

Rule of 150: A sample of at least 150 - 300 cases is recommended by Hutcheson and Sofroniou (1999). Cases more toward the 150 end when there are a few highly correlated variables are thus recommended.

Rule of 200: Guilford (1954) suggested that N should be at least 200 cases (in MacCallum, *et al*., 1999)

Rule of 250: Cattell (1978) claimed the minimum desirable N to be 250

Rule of 300: Tabachnick and Fidell (2014) suggest that a sample size of 300 for factor analysis is sufficient.

Rule of 500: Comrey and Lee (1999) thought that 100 = poor, 200 = fair, 300 = good, 500 = very good, 1,000 or more = excellent.

A summary of guidelines for the Subjects-to-variables (STV) ratios is presented as follows:

Subjects-to-variables (STV) ratio

Ratio of 20:1 – Hair *et al*. (1995) suggest that subjects-to-variables should at least be 20 subjects per variable.

Ratio of 10:1 – According to Nunnally (1967), there should be at least 10 cases for each item in the instrument being used.

Ratio of 5:1 - (Bollen, 1989; MacCallum, *et al*., 1999) suggest that the subjects-to-variables ratio should be no lower than 5.

Ratio of 3(:1) to 6(:1) of STV is acceptable if the lower limit of variables-to-factors ratio is 3 to 6. But, the absolute minimum sample size should not be less than 250 (Cattell, 1978).

Ratio of 2:1. Kline (1994) recommends at least twice as many subjects as variables in factor analytic investigations are required. Thus a minimum 100 subjects is suggested.

According to MacCallum, *et al*. (1999), literature has demonstrated that the general rule of thumb for the minimum sample size or STV ratio for factor analysis is not useful. Furthermore, Tabachnick and Fidel (2014) and Hair *et al.* (2014) suggest that the minimum level of sample size is dependent on other aspects such as the communality of the variables. If communalities are high, recovery of population factors in sample data is normally very good, almost regardless of sample size (Hair *et al.,* 2014).

In the current study, the sample size is 173. The central limit theorem assumptions were held for t-tests (see Section 7.5). Moreover, the sample size in this study falls under the rule of thumb 100-150 of the least number of cases required to perform factor analysis.

5.7 ETHICAL CONSIDERATIONS

According to Welman *et al*. (2005), ethical issues arise when the research involves human subjects. It is further suggested that the principles underlying 'research ethics' are universal issues such as honesty and respect for the rights of individuals, thus the subjects should take part in the study freely based on informed consent (Welma *et al*., 2005). Moreover, Creswell (2014) states that researchers need to protect their research participants, develop a trust with them, promote the integrity of the research and guard against misconduct that might reflect on their organisations. To address these issues, the ethics clearance was applied for and obtained from the University (Appendix C) permission from the relevant authority from where the target population and sample was requested (Appendix A) and obtained (Appendix B). Moreover, point 3 in the letter of authority (Appendix B) was complied with as indicated above in section 5.6.2. The other main ethical principles that were considered for conducting this study are respect for individuals in terms of informed consent and confidentiality/anonymity.

Ethical considerations included informed consent and confidentiality. Confidentiality was assured and maintained by allocating each participant with a number that was then used to link a particular participant to his/her dataset. Thus, the questionnaires were completed anonymous. Furthermore, the participants were informed of their rights as research participants and given the opportunity to ask questions and to opt out of the study at any time. Informed consent was also sought and signed for (Appendix D). In addition

5.7.1 Informed consent

According to Kumar and Phrommathed (2005), it is considered unethical in every discipline to collect information without the participant having expressed willingness and informed consent. Thus to ensure that informed consent is sought from participants, participants were adequately made aware of the type of information that was expected from them, the purpose and benefit of the study, how it will affect them, the expected duration, procedures as well as the proposed outcome. Moreover, it was emphasised that participation was voluntary and participants may withdraw from the study anytime during the research project.

5.7.2 Anonymity and confidentiality

To protect anonymity, the identifying information on the informed consent (Appendix D), letter of request (Appendix A) and authority to conduct the research (Appendix B) was removed. Furthermore, the self-administered paper questionnaires did not require participants to give any identifying information. According to Stangor (2011), in most cases data cannot be anonymous if the researcher needs to keep track of which participants contributed the data, which was the case in this study. Thus, it is proposed that participants can use unique code numbers to identify them as a solution that will respect their confidentiality (Stangor, 2011). In the context of this study, questionnaires were numbered by the researcher, thus a participant received a questionnaire corresponding to the numbered tag they received during the random assignment to groups, which was pinned as a name tag on them. This enabled the researcher to pair a dataset to a specific user to allow comparison during the data analysis phase.

5.8 SUMMARY

This chapter discussed the research methodology assumed in this study. The worldviews (paradigms) and research designs that were carried out to demonstrate the objective of this study were discussed. The next chapter discusses details of the data collection and analysis methods carried out in this study.

Chapter 6 : Data Collection and Analysis Methods

6.1 INTRODUCTION

In order to draw conclusions from any study, data needs to be collected Kumar and Phrommathed (2005). This chapter therefore provides the details of the empirical data collection methods and data analysis methods adopted in this study in Section 6.2 and 6.3, respectively. Furthermore, the validity and reliability of the research instrument is discussed in Section 6.4, and Section 6.5 summarises the chapter.

6.2 DATA COLLECTION PROCEDURES

The data was collected from three different locations, over the period of September to the beginning of November 2015 as the different areas are far apart. The researcher collected data from the participants by means of self-administered, structured questionnaires. According to Kumar and Phrommathed (2005), questionnaires are a list of written questions to which the answers are recorded by participants. The questionnaire approach allows larger groups of participants to complete comprehensive questionnaires, and can provide participants with a sense of anonymity, which can lead to trusted and valid responses (Stangor, 2011).

Kumar and Phrommathed (2005) propose different types of questionnaires categorised as follows:

- **Mailed questionnaires** which allow participants to complete and return the questionnaire by post at their own convenience.
- **Online questionnaires** use electronic mail or internet based survey questionnaire.
- **Collective questionnaires** allow a researcher to obtain a captive audience (i.e. assembling participants in one place), administer and collect the questionnaire by hand.

According to Creswell (2014), mailed and online questionnaire have an advantage of being filled out at the convenience of the participant; however, they tend to have a low response and usually require the researcher to email or phone participants as a reminder to complete the questionnaire. Since most of the participants in this study

did not have regular access to the internet or email, the collective questionnaire was seen as suitable to maximise the response rate. Kumar and Phrommathed (2005) suggests that collective questionnaire allows the researcher personal contact with the participants (e.g. the researcher is available to answer and clarify any queries immediately) which is absent when participants has to complete the questionnaire on their own (e.g online or via mail). Thus collective questionnaires were relevant for this study as they provided the researcher with the opportunity to confirm whether the questionnaire is totally completed.

Before distributing the questionnaires the researcher explained the nature and purpose of the study, thereafter informed consent was obtained. The study was divided into two phases running concurrently; phase one was the survey collecting data to determine end-users' current compliance behaviour and level of awareness training, whilst phase two was the experimental study consisting of a pre-test *and* post-test to test the theory of ISP awareness training influencing end-user attitudes towards ISP compliance. Both phases used questionnaires to obtain the data. Details of the different stages are discussed as follows:

6.2.1 Phase one: The Survey

The questionnaire used in this study consisted of questions regarding their demographics (see Appendix E, section A, part 1), including a set of questions to determine the current end-user's level of ISP awareness training and current compliance behaviour (Appendix E, section A Part 2). This questionnaire was completed by all the participants. Part 2 of section A consisted of thirteen questions, in which every construct was measured by several items.

6.2.2 Phase two: The experimental study

According to Oates (2006), an experimental study involves observations and making before and after measurements of the dependent variables; otherwise no change which might be attributed to the intervention on the independent variables can be observed. The different types of experimental design measurements as described by (Creswell, 2014) are discussed:

- **Post-test only control group design** - controls for any confounding effects of a pre-test, participants are randomly assigned to groups and an

intervention is only given to the experiment group, both groups are then measured on the post-test. If there is a difference one can be confident that it is attributable to the intervention. However, Field and Hole (2002) indicates that this design suffers from one weakness, i.e. if the random assignment of participants fails to produce equivalence, one cannot be certain that the two-groups were comparable before the intervention was administered.

- **Pre-test *and* Post-test control group design** - as with the previous design, the pre-test *and* post-test control group design uses two randomly assigned groups. Behaviour is then measured before and after the intervention for comparison. Any difference between the two conditions can be presumed to be due to the intervention administered to the experimental group. The advantage of this design over the previous one is that, because of the pre-test, one can be certain that the two-groups were equivalent before the intervention took place; however, the problem with this design is that pre-testing the participants may affect their subsequent performance as participants are already familiar with the questionnaire (Field and Hole, 2002). According to Field and Hole (2002), the Solomon four group design controls for the possibility of the above- mentioned problem.

- **Solomon four group design** – this design involves the random assignments of participants to the four groups. It consists of four conditions, two control and two experimental. Pre-tests and interventions are varied for the groups but all the groups receive a post-test. The advantage of this design is that, by making appropriate comparisons between the four conditions, one can assess the effects of pre-testing and therefore gain some idea of generalisability of the findings and eliminate the possibility that the cause of the change in one group is the pre-test and an intervention (Field and Hole, 2002). Although this is an excellent design, Field and Hole (2002) suggest that it is rarely used in practice due to being expensive and time consuming.

Therefore in the current study the pre-test *and* post-test control group design is seen most appropriate to determine the effect of the intervention on the experimental group so that any difference is attributable to the intervention. This will enable the

researcher to determine if ISP awareness training has an effect on end-users attitudes toward complying with their organisation‘s ISP.

The pre-test *and* post-test formed section B of the study and consisting of questions relating to attitude, self-efficacy and intentions to comply with the organisation’s ISP. The experiment kicked-off by administering the pre-test together with Section A to both groups, after which the control group left the venue. The experimental group was then exposed to an awareness (ISP awareness video) produced by the organisation to address the specific information security policy requirements and guidelines in the organisation. The video showed what constituted inappropriate behaviour and what risks such behaviour can cause as well as end-users’ roles and responsibilities regarding actions they can take to be more information security conscious. The awareness videos addressed topics such as password security, backups, encryption, virus control, security education, email and internet usage. At the end of the video key messages were recapped to summarise the main points of the video.

In conjunction with the awareness video, a brief lecture on ISP security basics and literacy training that was created by the researcher was presented. Puhakainen and Siponen (2010) suggest that, when providing IS security training, learning tasks that are of personal relevance to the learners should be used so that there are visible consequences. Therefore a customised approach was used to provide end-users with appropriate content (e.g. a subset of behaviours based on the organisation’s ISP). The aim of the lecture was to define security concepts and how these concepts should be applied. According to the (NIST, 1998), the security basics and literacy training provides the foundation for subsequent role-based training by providing a universal baseline of key security terms and concepts so that end-users are familiar with the “IT security basics” core knowledge set, and have the ability to apply these knowledge sets to protect electronic information and systems. Moreover, the (NIST, 2003) specifies that an awareness training explains proper rules of behaviour for the use of the organisation’s and communicates information security policies and procedures that needs to be followed. Hence this study integrates awareness and training as one tool to communicate and explain the ISP.

In order to measure the effect of an intervention, Kumar and Phrommathed (2005) suggests collecting two sets of data at two points in time on the same population. Furthermore, the (NIST, 2003) proposes that organisations can evaluate their training programmes by ascertaining end-user attitudes toward computer security and how much information is retained after such programmes, as the results of such evaluations could help identify and correct problems. Some popular strategies proposed by the publication are using trainee evaluations to collect feedback and testing employees on material soon after it has been covered in training. However, Herold (2010) proposes a follow up evaluation approximately 4-6 months after the training to determine how well end-users have retained the information. Some other studies measuring attitudes after an intervention conducted the post-test immediately; others 1 month after the intervention and some measured attitudes immediately and 1 month after the intervention to observe any variation over time (Ghaffari *et al*., 2013; Hanafi *et al*., 2014; Wong *et al*., 2015).

In the current study end-users' attitudes toward ISP compliance was measured immediately after the intervention to assess the effect of ISP awareness training. Both groups completed a post-test soon after the experimental group was exposed to the intervention. The same questionnaire which was completed during the pre-test was administered as the post-test. All the measurement items on the tests were based on a 5-point Likert scale ranging from "strongly disagree" (1) to "strongly agree" (5) in which participants were asked to indicate an appropriate response. The complete set of measuring items is provided as Appendix E. The data collected was analysed using statistical data analysis techniques.

6.3 DATA ANALYSIS PROCEDURES

According to Oates (2006), quantitative analysis is mainly used for the type of data generated by surveys and experiments. As this study conducts both the survey and an experiment, the data analyses associated with quantitative strategies are discussed in the following sections. Welman *et al*. (2005) discusses two types of statistics which are applied in this study:

- The survey, which in this study provides descriptive statistics for the description or summary of the data obtained from participants. The data is

furthermore grouped and presented in the form of tables and graphical distributions.

- Inferential statistics are used for the experimental study to make inferences about population indices obtained from samples drawn randomly and involve using analysis of variances such as parametric and non-parametric tests to test hypotheses.

Furthermore, a statistician analysed the data using the Statistical Package for Social Sciences (SPSS) version 23. The following section discusses and explains the credibility of the research instrument used to collect data in this study.

6.4 RELIABILITY AND VALIDITY

Reliability is the degree of accuracy or precision in the measurements made by a research instrument (Welma et al., 2013), whilst the concept of validity refers to the extent to which a measured variable actually measures the conceptual variable (Stangor, 2011). According to Adams and Lawrence (2015) reliability is the prerequisite of validity, as validity alone cannot demonstrate its strength. In other words, reliability and validity are both required to measure variables.

6.4.1 Reliability Measurement of the research Instrument

According to Kumar (2014), the concept of reliability in relation to a research instrument is when the research tool is consistent and stable, and therefore predictable and accurate. Thus the greater the degree of consistency and stability in an instrument, the greater its reliability will be (Kumar, 2014). To test reliability of the questionnaire, item analysis was done on the questionnaire to determine Cronbach alpha values. According to Welma *et al*. (2005), Cronbach's alpha is used to check for the degree to which all the items in a measurement measure the same attribute. Cronbach alpha is used to determine how unified the items in the dimension are by measuring the internal consistency of each dimension (Salkind, 2012).

Revelle and Zinbarg (2009) provided the following rules of thumb that if it is ≥ .9 – excellent, ≥ .8 – good, ≥ .7 – acceptable, ≥ .6 questionable, ≥ .5 poor and < .5 unacceptable. In order for a scale to be considered internally consistent an alpha of .7 or higher (≥.7) is desired, although slightly below (.6) is also usually considered acceptable (Nunnally, 1967; Adams and Lawrence 2015). This is also concurred by

Hair *et al*. (2014), who indicated that the general agreed lower limit is .7 and in exploratory research it might decrease to .6. In this research .7 was used as an acceptable level. The reliability is given in Table 6-1.

Table 6-1: Reliability Results of Dimensions

Aspect	No. of items	Cronbach's alpha	Acceptable level
Level of information security policy awareness training	9	.897	Good
Current behaviour	5	.741	Acceptable
Overall survey questionnaire	**14**	**.903**	**Excellent**
Attitudinal	5	.905	Excellent
Self-efficacy	7	.890	Good
Intention to comply with the information security policy	5	.903	Excellent
Overall pre-experimental instrument	**17**	**.910**	**Excellent**
Attitudinal	5	.948	Excellent
Self-efficacy	7	.941	Excellent
Intention to comply with the information security policy	5	.958	Excellent
Overall post-experimental instrument	**17**	**.955**	**Excellent**
Total	**48**	**.957**	**Excellent**

It can be noted that all dimensions achieved the minimum threshold as proposed by Hair *et al*. (2014.) The overall reliability of the instrument was .957 which is excellent and it can be concluded that the instrument was very reliable.

6.4.2 Validity Measurement of the research Instrument

Validity is defined as the ability of an instrument to measure what it is designed to measure (Creswell, 2014) and refers to the extent to which a measured variable actually measures the conceptual variable (Stangor, 2011). Adams and Lawrence (2015) and Cohen, Manion and Morrison (2011) propose two types of validity to be examined, namely internal and external validity.

Internal validity applies when a researcher examines causal relationship, thus internal validity is seen as the extent to which it can be assumed that the results from a study is in fact caused by the manipulation of the independent variable (Adams and Lawrence, 2015). Furthermore, it is suggested that researchers can choose one type of validity over the other, depending on one's particular interest, i.e. if a

researcher examines the effect of a variable or procedure, then the focus may be on internal validity, whereas another researcher who is more interested in finding out how well a finding established in one setting generalises to another setting may focus on external validity. Otherwise “researchers must find balance between internal and external validity, so that they are confident the independent variable is responsible for the changes in the dependent variable and that the findings are generalizable to other situations or populations” (Adams and Lawrence, 2015).

The following efforts to maximise internal validity in this study were adopted as proposed by Adams and Lawrence (2015):

- The independent variable condition was the only factor that varied across the groups.
- Participants were randomly assigned to the independent variable condition to ensure that the groups are similar prior to exposure to the IV manipulation (ISP awareness training or no ISP awareness training).
- An awareness video and a power point lecture were used to ensure that the lecture content was exactly the same for all participants.

According to Adams and Lawrence (2015), efforts adopted to maximise internal validity may reduce external validity, thus a relatively large sample is proposed. The sample size in this study is relatively large as discussed in section 5.6.3.

Furthermore, Adams and Lawrence (2015) suggest that the validity of the test results can be enhanced by collecting quantitative data with which statistical analysis can be performed and by using different evaluation methods, discussed below.

Face validity refers to the extent to which the measured variable appears to be an adequate measure of the conceptual variable (Stangor, 2004) to check whether the questionnaire seems to measure the concept being tested. Kumar and Phrommathed (2005) indicates that just as face validity is the judgement of whether an instrument is measuring what it is supposed to, it is equally important that the items and questions cover the full range of the issue being measured. The assessment of the items of an instrument in this respect is called content validity (Kumar and Phrommathed, 2005).

Content validity is also judged on the basis of the extent to which statements or questions represent the issue they are supposed to measure, as judged by the researcher and experts in the field (Kumar and Phrommathed, 2005). The judgement is based on the subjective logic as no objective method exists. Cornford and Smithson (2006) suggest that it is usually essential to carry out one or more test runs with any questionnaire, to ensure that questions are understandable Therefore, to test for face and content validity of the instrument, friends and colleagues were asked to test run the instrument to see if questions were relevant and understandable.

Criterion validity relates scores from a scale to a current or future behaviour that represents the construct measured by the scale (Adams and Lawrence, 2015).

Construct validity is whether a measure mirrors the characteristics of a hypothetical construct, i.e. how the scale measures or correlates with the construct that it attempts to measure.

According to Cohen *et al.* (2011), construct validity is addressed by convergent and discriminant (divergence) techniques. Convergent validity is demonstrated when two related or similar factors of a particular construct are shown to be related or similar to each other (Cohen *et al.,* 2011). Convergent validity was used in this study to test constructs for convergence or divergence (discriminant) on the decision variables with factor loadings. To test the convergent validity of all the dimensions in the questionnaire, factor analysis was carried out to determine whether the individual questions contributed to their respective constructs.

There are two types of factor analysis: exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) (Pallant, 2010). The validity of the instrument was measured using exploratory factor analysis. Factor analysis is an interdependence technique whose primarily purpose is to define the underlying structure among the variables in the analysis (Hair *et al*., 2014). According to Kline (1994), factor analysis is performed to determine if individual questions load or contribute onto the construct as in the questionnaire. Thus a set of highly inter-correlated measured variables will be grouped into distinct factors. The method used was the principal component analysis with a varimax rotation. The number of factors to be retained in the factor

solution where determined using the latent root criterion which is one of the mostly used methods for determining the number of factors to be retained. According to Hair *et al*. (2014), this technique is simple to apply to either component analysis or common factor analysis. The authors indicated that only the factors having latent roots or eigenvalues more than one are considered significant.

The appropriateness of the factor analysis is measured using the Kaiser-Meyer Olkin (KMO) and Bartlett Test of Sphericity. The KMO is a measure of sampling adequacy that is used to quantify the degree of intercorrelation among the variables and it ranges from 0 to 1. The measure can be interpreted with the following guidelines: .8 or above, meritorious; .7 and above, middling; 0.6 and above, mediocre; .5 or above, miserable; and below .5 unacceptable (Hair *et al*., 2014). The researcher should always have an overall measure of sampling adequacy of above .5 before proceeding with factor analysis (Tabachnick and Fidell, 2014; Hair *et al*., 2014). In terms of the eigenvalues, which account for the variance in a particular dataset, Kaiser's criterion can be used as a rule of thumb to determine the number of factors to be retained. This criterion suggests retaining all factors that are above the eigenvalue of 1 (Kaiser, 1960). According to Pallant (2010), the factor solution is robust if the amount of variance explained is at least 50%. In terms of communalities there should be values above .5 or most of the variables should have communalities above .6. (Pallant, 2010)

The Bartlett Test of Sphericity tests whether the correlations among variables are too low for the factor model to be appropriate (Dugard, Todman and Staines, 2010). The null hypothesis of lack of sufficient correlation is rejected if the p-value is less than .05 (Tabachnick and Fidel, 2014; Hair *et al*., 2014).

Thus factor analysis was done using principal component analysis with varimax rotation to show the factors that are correlated with one another. According to Adams and Lawrence (2015), factor loadings are regarded as high and meaningful if they are greater than .5 (the positive or negative sign is irrelevant), and moderately high if they are above .3, while other loadings are ignored.

Factor analysis on the survey instrument

The aspects "*Level of ISP Awareness Training Question9* (*LISPAT9_B.), Information Security Policy training in my organisation helps me to understand how to behave appropriately towards matters related to information security*" and "*Current Compliance Behaviour Question2* (*CB2_B.), I tend to comply with the Information Security Policy only when it is convenient to do so*" were dropped from the analysis due to insignificant factor loadings below .5. The factor solution is shown in Table 6-2.

Table 6-2: Rotated Factor Solution for Survey Instrument

Factors and observed variables	**Loadings**	**Eigen values**	**% of variance**
Factor 1: Level of ISP Awareness Training		3.219	26.82%
LISPAT3_B. I know the rules and regulations prescribed by the Information Security Policy of my organisation.	.810		
LISPAT4_B. I understand the rules and regulations prescribed by the Information Security Policy of my organisation.	.782		
LISPAT2_B. I keep myself updated in terms of information security awareness.	.751		
LISPAT5_B. I know my responsibilities as prescribed in the Information Security Policy to enhance the IS security of my organisation.	.726		
LISPAT1_B. I am aware of potential information security threats.	.624		
Factor 2: Current Compliance Behaviour		3.067	25.56%
CB5_B. I recommend others to comply with information security policy.	.843		
CB4_B. I assist others in complying with information security policy.	.789		
CB1_B. I comply with the Information Security Policy when performing my daily work.	.723		
CB3_B. I practice recommended information security behaviour as much as possible.	.657		
Factor 3: Level of ISP Awareness Training		2.334	19.45%
LISPAT7_B. The management organises information security training effectively.	.872		
LISPAT8_B. The management encourages me to attend the information security trainings.	.830		
LISPAT6_B. The management updates me on the changes related to the Information Security Policy.	.668		
Total variance explained			**71.83%**

The principal component analysis with a varimax rotation resulted in a KMO of .872 with a Bartlett Test of Sphericity that gave a p-value of .000. Thus the solution was appropriate for factor analysis and since KMO was above .5 the Bartlett's Test of Sphericity was significant. The communalities ranged from .534 to .859 and most of them were above .6. The factor solution resulted in a two-factor solution as shown in Table 6-2 above. Thus three factors were retained. The amount of variability explained by three factor solutions was 26.82%, 25.56% and 19.45%, respectively. Thus the factor solution was robust since the amount of variability accounted for was 71.83%.

Factor analysis on pre-experimental instrument

A three-factor solution was obtained. The KMO measure of sampling adequacy was .887 whilst the Bartlett test of Sphericity had a significant p-value = .000. Thus there was sufficient correlation between variables and the Kaiser-Meyer-Olkin (KMO) measure of sampling indicated that the correlations are adequate for factor analysis. The majority of the communalities were above .6.

The factor solution put the factors into their original sections which are attitudinal, self-efficacy and intention to comply. The first factor had an eigenvalue of 4.125, accounting for 24.26% of the total variance. The second factor had an eigenvalue of 3.950, accounting for 23.24 of the total variance and the third factor had an eigenvalue of 3.737, accounting for 21.93% of the total variance. Altogether the variables accounted for 69.42% of the total variance.

The factor solution is shown in Table 6-3.

Table 6-3: Rotated Factor for Pre-experimental Instrument

Factors and observed variables	Loadings	Eigen values	% of variance
Factor 1: Attitudinal		4.125	24.26%
SEFY4_B. I have the necessary skills to protect myself from information security violations.	.867		
SEFY2_B. I have the necessary knowledge to fulfil the requirements of the ISP.	.840		
SEFY1_B. I have the necessary skills to fulfil the requirements of the ISP.	.822		
SEFY5_B. I have the expertise to implement preventative measures to stop people from getting my confidential information.	.814		
SEFY6_B. It is easy for me to enable security features on my work computer by myself.	.708		
SEFY3_B. I can use information security measures if I can call for help if I get stuck.	.573		
SEFY7_B. I believe that it is within my control to protect myself from information security violations.	.550		
Factor 2: Self-efficacy		3.950	23.24%
INT3_B. I am likely to follow the organisation's ISP in the future.	.864		
INT5_B. I am certain I will adhere to my organisation's ISP.	.847		
INT4_B. I would follow the organisation's ISP whenever possible.	.812		
INT2_B. I intend to assist others in complying with information security policies.	.749		
INT1_B. I intend to comply with information security policies.	.679		
Factor 3: Intention to comply		3.727	21.93%
ATT3_B. Following the organisation's ISP is a good idea.	.856		
ATT1_B. I feel that compliance to information security policies is a positive thing.	.802		
ATT2_B. I feel that compliance to information security policies is important.	.801		
ATT4_B. Information security policy helps secure computer systems.	.774		
ATT5_B. Following the organisation's ISP is a necessity.	.731		
Total variance explained			**69.42%**

Factor analysis on post-experimental instrument

The aspect *"SEFY7_B., I believe that it is within my control to protect myself from information security violations"* was dropped due to cross loadings, Tfactor solution resulted in a two factor. The Bartlett's Test of Sphericity had a chi-square value = 3133.845 with a p-value =.000 leading to the rejection of the null hypothesis of lack

of sufficient correlation between variables. The KMO measure of sampling adequacy was .931, indicating that the correlations are adequate for factor analysis. The communalities ranged from .668 to .839. The factor solution is shown in Table 6-4.

Table 6-4: Rotated Factor Solution for Post-experimental Instrument

Factors and observed variables	Loadings	Eigen values	% of variance
Factor 1: Attitudinal and intentions to comply		7.519	47.00%
INT2_A. I intend to assist others in complying with information security policies.	.882		
INT1_A. I intend to comply with information security policies.	.872		
ATT3_A. Following the organisation's ISP is a good idea.	.869		
INT4_A. I would follow the organisation's ISP whenever possible.	.868		
ATT1_A. I feel that compliance to information security policies is a positive thing.	.847		
ATT5_A. Following the organisation's ISP is a necessity.	.842		
ATT2_A. I feel that compliance to information security policies is important.	.832		
INT5_A. I am certain I will adhere to my organisation's ISP.	.823		
ATT4_A. Information security policy helps secure computer systems.	.806		
INT3_A. I am likely to follow the organisation's ISP in the future.	.794		
Factor 2: Self-efficacy		4.865	30.41%
SEFY1_A. I have the necessary skills to fulfil the requirements of the ISP.	.897		
SEFY2_A. I have the necessary knowledge to fulfil the requirements of the ISP.	.897		
SEFY4_A. I have the necessary skills to protect myself from information security violations.	.860		
SEFY6_A. It is easy for me to enable security features on my work computer by myself.	.819		
SEFY5_A. I have the expertise to implement preventative measures to stop people from getting my confidential information.	.812		
SEFY3_A. I can use information security measures if I can call for help if I get stuck.	.760		
Total variance explained			**77.40%**

The factor solution grouped two of the original sections into 1. The factors were named attitudinal, intentions to comply and self-efficacy. The first factor had an eigenvalue of 7.519, accounting for 47.00% of the total variance and the second

factor had an eigenvalue of 4.865, accounting for 30.41% of the total variance. Altogether the variables accounted for 77.40% of the total variance.

6.5 SUMMARY

This chapter discussed the data collection and analysis methods adopted in this study to answer the research questions. The construction, validity and reliability of the research instrument was also presented and explained. The next chapter thus present the data analysis and interpretation.

Chapter 7 : Research Analysis and Interpretation

7.1 INTRODUCTION

This chapter presents the analyses of the quantitative data. The aim of the study was to seek to propose and empirically validate a model and to assess the significance of ISP awareness training on influencing end-user attitudes towards complying with their organisation's ISP. To achieve this objective, the researcher found out the current level of end-user's ISP awareness and their ISP compliance behaviour and tested the influence of ISP awareness training on end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP. The results were correlated with existing literature.

The quantitative data collected was analysed using descriptive statistics in the form of proportions, frequencies, means and standard deviations, independent t- tests and paired t-tests to compare differences between two-groups and Analysis of Variance (ANOVA) to compare difference between more than two-groups. For the interaction effects that were significant, graphical illustrations are used to explain such effects.

The results obtained in this study are presented and discussed below. The sequence of the presentation and the discussion of the results are in accordance with the hypotheses formulated for the study. The hypotheses of the study are outlined in Table 7-1. The chapter commences with the demographics in Section 7.2, followed by the descriptive analysis of the survey and the experiment in Section 7.3 and 7.4, respectively.

Table 7-1: Hypotheses to be tested

Hypothesis 1	H_0:	ISP Awareness training does not affect an employee's attitude to comply with their organisation's ISP
	H_1:	ISP Awareness training directly affects an employee's attitude to comply with their organisation's ISP
Hypothesis 2	H_0:	ISP Awareness training does not affect an employee's self-efficacy to comply with their organisation's ISP.
	H_1:	ISP Awareness training positively affects an employee's self-efficacy to comply with their organisation's ISP.
Hypothesis 3	H_0:	Self-efficacy has no influence on end-users' attitudes toward complying with their organisation's ISP

	H_1:	Self-efficacy has a positive influence on end-users' attitudes toward complying with their organisation's ISP
Hypothesis 4	H_0:	Self-efficacy has no impact on end-users' intention to comply with their organisation's ISP
	H_1:	Self-efficacy has a positive impact on end-users' intention to comply with their organisation's ISP
Hypothesis 5	H_0:	The end-users' attitude towards complying with their organisation's ISP has no impact on their intention to comply
	H_1:	The end-users' attitude towards complying with their organisation's ISP has a positive impact on their intention to comply

The next section presents the results characterising the sample per area. The entire sample comprised end-users within a government organisation in the North West province.

7.2 DEMOGRAPHIC CHARACTERISTICS OF THE SAMPLE

A total of 173 end-users of the ABC government agency participated in the study. The demographic characteristics of the participants are given below. In terms of location, there were 22.0% (n=38) participants from Mafikeng, 68.8% (n=119) from Potchefstroom and 9.2% (n=16) from Zeerust. Thus the majority of the participants were from Potchefstroom. This may be attributed to the fact that Potchefstroom was the largest strata.

Furthermore Table 7-2 presents the characteristics of the end-users by gender and Table 7-3 presents characteristics of end-users by level of computer use.

Table 7-2: Characteristics of the end-users by gender

		Location			
Variable		**Mafikeng**	**Potchefstroom**	**Zeerust**	**Total**
Gender	Male	68.4% (26)	63.8% (64)	62.5% (10)	57.8% (100)
	Female	31.6% (12)	46.2% (55)	37.5% (6)	42.2% (73)
	Total	**22.0% (38)**	**68.8% (119)**	**9.2% (16)**	**100% (173)**

In terms of gender, the majority were males comprising 57.8% (n=100) and 42.2% (n=73) were females. In all locations a predominance of males over females is evident. In Mafikeng the males comprised 68.4% (n=26) whilst the composition of females was 31.6% (n=12), in Potchefstroom the males comprised 53.8% (n=64)

and 46.2% (n=55) for females and in Zeerust 62.5% (n=10) were males whilst 37.5% (n=6) were females. It can be observed that in Potchefstroom, the ratio of males to females is almost 1:1. Thus there is a fairly equal distribution of males and females.

Table 7-3: Characteristics of end-users by Level of Computer use

		Location			
Variable		**Mafikeng**	**Potchefstroom**	**Zeerust**	**Total**
Level of Computer use	Under 1 year	2.6% (1)	7.6% (9)	18.8% (3)	7.5% (13)
	1 – 3 years	15.8% (6)	19.3% (23)	25.0% (4)	19.1% (33)
	4 – 6 years	21.1% (8)	26.9% (32)	31.3% (5)	26.0% (45)
	7 – 9 years	26.3% (10)	16.8% (20)	6.3% (1)	17.9% (31)
	More than 10 years	34.2% (13)	29.4% (35)	18.8% (3)	29.5% (51)
	Total	**22.0% (38)**	**68.8% (119)**	**9.2% (16)**	**100% (173)**

Additionally, participants were asked to indicate how frequently they have been using a computer in their organisation. About 29.5% (n=51) had been using them for more than ten years, 26.0% (n=45) for 4 – 6 years, 19.15 (n=33) for 1 – 3 years, 17.9% (n=31) for 7 – 9 years whilst 7.5% (n=13) where under 1 year. Thus the majority of the participants have been using a computer as evidenced by the fact that 73.3% have been using a computer for more than three years with close to 50% using it for more than 6 years. In terms of the work location areas, in Mafikeng 26.3% (n=10) have been using a computer for 7 – 9 years and 34.2% (n=13) for more than 10 years. Thus 60.3% have been using a computer for more than 6 years. Similarly, in Potchefstroom, 16.8% (n=20) have been using a computer for 7 – 9 years and 29.4% (n=35) for more than 10 years. Thus close to 50% have been using a computer for more than 6 years. It was also observed that 26.9% (n=32) have been using a computer for 4-6 years. One can conclude that in Potchefstroom the majority of the participants, that is, close to 75% have been using a computer for more than 4 years. For Zeerust the scenario is different in that only 25.1% (n=4) have used a computer for more than 6 years with 31.3% (n=5) using it for 4 – 6 years and 25.0%

(n=4) for 1 – 3 years. One can conclude that the level of computer use is high in Mafikeng, followed by Potchefstroom and then lastly Zeerust.

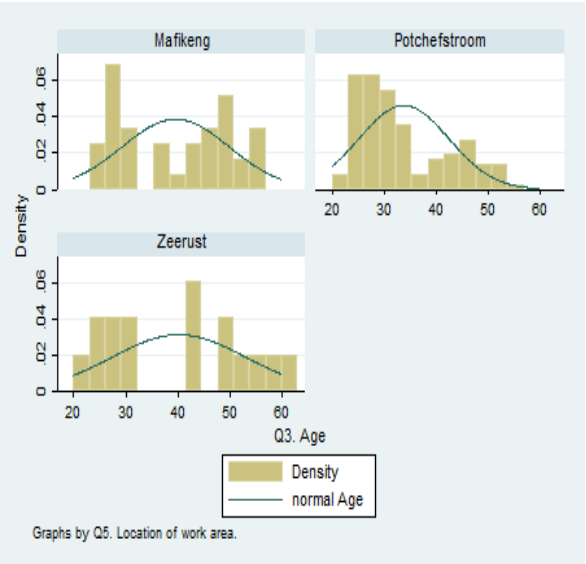
The mean, median and mode of the age of the participants were 35.55 years, 32.00 years and 28.00 years as shown in Table 7-4.

Table 7-4: Summary statistics of age in years

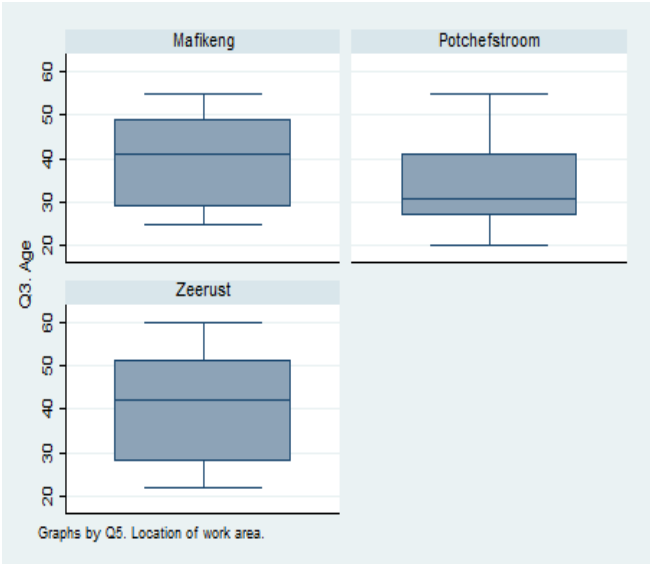
Summary Statistics	Mafikeng	Potchefstroom	Zeerust	Overall
Mean	39.55	33.79	40.19	35.55
Median	41.00	31.00	42.00	32.00
Mode	28.00	26.00	42.00	28.00
Standard deviation	10.292	8.614	12.760	9.776
Skewness	-.033	.775	.098	.581
Kurtosis	-1.610	-.601	-1.501	-.970
Maximum	55	55	60	60
Minimum	25	20	22	20
Range	30	35	38	40
Coefficient of variation	26.02%	25.49%	31.75%	27.50%

It can be noted that 68.26% (± one standard deviations from the mean) are between 25.77 years and 45.33 years old. Thus one can conclude that overall most of the participants are middle aged. The coefficient of variation was 27.5% which indicates that there is not much variability since it is close to zero.

In Mafikeng the average age is 39.55 with a standard deviation of 26.02%. Thus 68.26% of the participants are aged between 29.26% years and 49.94 years. For Potchefstroom the mean and the median were 33.79 years and 31 years, respectively with a standard deviation of 8.614 and 68.26% of the participants were aged between 25.18 and 42.40 years. The work area with the highest average age was Zeerust. The mean and median were 40.19 years and 42 years, respectively. About 68.26% of the participants had average age between 27.43 years and 52.95 years. The standard deviation was 12.760 with a coefficient of variation of 31.75%. It was the one with the highest variability as evidenced by the highest coefficient of variation. The pattern can be depicted in the histograms and box plots in Figure 7-1.



Sub-Figure 7-1-1: Histogram



Sub-Figure 7-1-2: Histogram

Figure 7-1: Histograms and box plots showing age of participants

All histograms showed that they are not normally distributed. On sub-figure 7-1-1, Zeerust seem to be having two-groups of participants. One group is aged above 40 years and the other group at most 30 years. Looking at the boxplots in sub-figure 7-1-2, Mafikeng data seem to be negatively skewed, whilst Potchefstroom data is positively skewed and Zeerust data is negatively skewed. Thus there is no area with age groups that are normally distributed. Looking at the distribution of Zeerust one can conclude that most of the people are above 40 years and this is the location which had lower levels of usage of computers.

In terms of tenure (years working in the organisation), the mean, median and mode are 14.60 years, 12.580 and 7.0 years, respectively. Thus looking at all the participants, at least 50% had more than 12.5 years in the organisation as shown in Table 7-5.

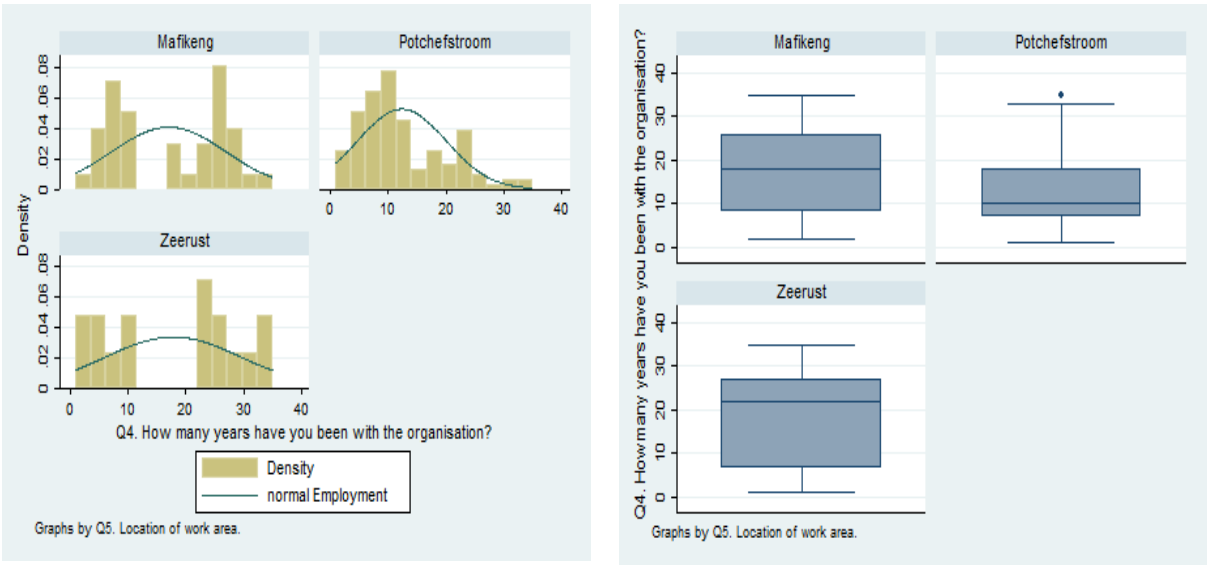
Table 7-5: Summary statistics of years working in the organisation

Summary Statistics	Mafikeng	Potchefstroom	Zeerust	Overall
Mean	17.03	12.37	17.81	14.60
Median	18.00	10.00	22.00	12.50
Mode	7	7	1	7
Standard deviation	9.783	7.582	11.783	8.644
Skewness	.054	.831	-.123	.393
Kurtosis	-1.514	.046	-1.584	-.978
Maximum	35	35	35	35
Minimum	2	1	1	1
Range	33	34	34	34
Coefficient of variation	57.45%	61.29%	66.16%	59.21%

Mafikeng is the area with high levels of staff retention as evidenced by tenure of 17.03 years with a median of 18 years. The coefficient of variation is 57.45%, giving the ratio of the standard deviation to the mean as 57:100. For Potchefstroom the mean and median are 12.37 years and 10 years, respectively. This is the work area with the lowest staff retention.

Zeerust has a mean of 17.81 and a median of 22.00 years. It is the work area with the highest levels of staff retention as compared to the other areas. However, it is the one with the highest coefficient of variation of 66.16%, indicating that Zeerust had the most variation it terms of staff retention such that the ratio of the standard deviation to the mean is 66:100. The pattern can be depicted in the histograms and box plots in Figure 7-2.

A mode of 1 can also be observed in Table 7-5 for Zeerust, indicating that most end-users have been working for the organisation for just about a year; however, when comparing these results with other areas, one could identify the mode for Zeerust as an outliner, which could be attributed to the small sample in Zeerust. According to Manikandan (2011) the mode is rarely used in small samples as the fluctuation in the frequency of observation is more (i.e. it is more likely that two or more people can have the same response in a small sample).



Sub-Figure 7-2-1: Histogram

Sub-Figure 7-2-2:Box Plot

Figure 7-2: Histograms and box plots showing years in the organisation of participants

Looking at figure 7-2, all histograms were not normally distributed as shown on sub-figure 7-2-1. Mafikeng and Zeerust seem to be having two groups of participants. Sub-figure 7-2-2 shows the boxplot, which indicates Mafikeng appearing to be normally distributed whilst those for Potchefstroom and Zeerust seem to be negatively skewed. Although a mode of 1 was observed for Zeerust, one can still conclude that the majority of the people in Zeerust have been working in the organisation for a long time as this is supported by the highest coefficient of variation of 66.16% as mention above.

Having discussed the demographics of the participants, the analysis of the survey results follows.

7.3 DESCRIPTIVE ANALYSIS OF THE SURVEY QUESTIONNAIRE

The analysis of the survey answers this research question:

- *What is the current level of end-users' ISP awareness training and their ISP compliance behaviour?*

The survey scale used in this study to measure end-users' level of ISP awareness training and compliance behaviour was developed and used by Bulgurcu *et al*. (2010), Martin and Rice (2011) and Siponen *et al*. (2014). This scale consist of 14 items, 9 of which address questions regarding the level of ISP awareness training and 5 addressing end-users' current compliance behaviour. The data set is analysed to determine the overall level of ISP awareness training and compliance behaviour of the entire organisation sample. The results were analysed in such a way that strongly agree was given a score of 5, agree 4, neutral 3, disagree 2 and strongly disagree 1. Strongly agree and agree were collapsed together to give the level of agreement whilst strongly disagree and disagree gave the level of disagreements. According to (Chawla & Sadhi, 2015 and De Vause, 2001), it might be essential for a researcher to combine adjacent categories of variables with similarity (e.g. strongly agree & agree and/or strongly disagree & disagree). This is to measure how greater the odds are for a member of a certain group to fall into a certain set of categories (i.e. strongly agree & agree and/or strongly disagree & disagree) than the odds are for a member of another group to fall in the same set of categories. The items were then ranked using the mean. Table 7-6 below summarises the key outcomes of the mean.

Table 7-6: Summary of key outcomes

Mean	Level of Agreement
3.5 and above	Agree
2.5 to 3.4	Neutral
below 2.5	Disagree

7.3.1 Descriptive statistics for level of ISP awareness training

There were 9 items addressing questions regarding the current level of ISP awareness training. Items were then ranked by Mean in order to show the highest to lowest agreement which end-uses agreed with the most, a mean of 1 indicates the highest level of agreement and 9 the lowest. The items are shown in Table 7-7.

Table 7-7: Level of agreement on aspects on level of Information Security Policy awareness training

Statement	Level of agreement			Mean	Rank
	Agree	Neutral	Disagree		
LISPAT1_B. I am aware of potential information security threats.	87.3% (151)	5.8% (10)	6.9% (12)	4.09	1
LISPAT9_B. Information Security Policy training in my organisation helps me to understand how to behave appropriately towards matters related to information security.	75.1% (130)	13.3% (23)	11.6% (20)	3.84	2
LISPAT5_B. I know my responsibilities as prescribed in the Information Security Policy to enhance the IS security of my organisation.	72.3% (125)	12.7% (22)	15.0% (26)	3.72	3
LISPAT8_B. The management encourages me to attend the information security trainings.	69.4% (120)	13.3% (23)	17.3% (30)	3.71	4
LISPAT3_B. I know the rules and regulations prescribed by the Information Security Policy of my organisation.	64.2% (111)	16.8% (29)	19.1% (33)	3.60	5
LISPAT4_B. I understand the rules and regulations prescribed by the Information Security Policy of my organisation.	68.2% (118)	10.4% (18)	21.4% (37)	3.57	6
LISPAT2_B. I keep myself updated in terms of information security awareness.	69.4% (120)	10.4% (18)	20.2% (35)	3.53	7
LISPAT7_B. The management organises information security training effectively.	53.2% (92)	19.1% (33)	27.7% (48)	3.32	8
LISPAT6_B. The management updates me on the changes related to the Information Security Policy.	55.5% (96)	16.8% (29)	27.7% (48)	3.29	9

The results show that 87% of end-users agree with the aspect LISPAT1_B, whilst 75% agree with LISPAT9_B. This findings show that end-users, who are aware of security threats, tend to believe that training helps them to understand how to behave appropriately towards matters related to information security. This view is consistent with the notion that suggests that employees who are aware of security issues are ideally committed to the security objectives of their organisation (Bulgurcu *et al.,* 2010).

In general, 69% of end-users agree that they keep themselves updated in terms of information security awareness. More so that 72% of end-users agree with the aspect LISPAT5_B and 68% agree with LISPAT4_B. . Based on the high level of

agreement from the respondents it can be concluded that end-users know and understand their responsibilities in terms of their organisation's ISP.

Knapp and Ferrante (2012) recommend awareness enhancing activities to include security briefings, formal training, regular reminders and promulgation of organisational ISP to ensure the implementation of information security. Although 69% of end-users in the current study agree with LISPA8_B, the results still show that more can be done in terms of management organising such security trainings and updating end-users on the changes related to the organisation's ISP. As only 55% of end-users agree with the aspect LISPAT6_B and 53% agree with LISPAT7_B. Moreover, the results demonstrate that the support of managers in delivering information security awareness and training is of paramount importance. Accordingly, management support in information security initiatives has been called for in literature (Siponen *et. al.,* 2014; Soomro, Shah and Ahmed, 2016).

7.3.2 Descriptive statistics for current Compliance behaviour.

There were 5 items addressing end-users' current compliance behaviour. The results of the items are shown in Table 7-8.

Table 7-8: Level of agreement on aspects of current behaviour

Statement	Level of agreement			Mean	Rank
	Agree	Neutral	Disagree		
CB1_B. I comply with the Information Security Policy when performing my daily work.	76.3% (132)	15.6% (27)	8.1% (14)	3.89	1
CB3_B. I practice recommended information security behaviour as much as possible.	78.6% (136)	15.0% (26)	6.4% (11)	3.87	2
CB5_B. I recommend others to comply with information security policy.	76.9% (133)	9.8% (17)	13.3% (21)	3.80	3
CB4_B. I assist others in complying with information security policy.	64.2% (111)	18.5% (32)	17.3% (30)	3.57	4
CB2_B. I tend to comply with the Information Security Policy only when it is convenient to do so.	37.0% (64)	17.9% (31)	45.1% (78)	2.85	5

With regard to the end-users' current ISP compliance behaviour, the results shows that majority of end-users comply with their organisations ISP, so much so that most

of the end-users (45%) disagreed with the contradicting statement CB2_B. Looking at the results, 79% of end-users agree with the CB3_B statement while 77% agree with CB5_B. Furthermore, 76% of end-users agree with CB1_B statement and 64% agree with statement CB4_B. When looking at the results one can conclude that end-users not only do they comply with their organisational ISP but they also assist others with complying with the ISP by recommending. Thus, it can be inferred that the organisation's current information security culture is positive. The information security culture is defined as the perceptions and attitudes accepted and encouraged to incorporate information security as the way things are done in an organisation (Da Vieiga, Martins and Eloff, 2007).

Moreover due to the fact that information security culture is learned, Da Veiga and Eloff (2014) propose that management can promote and encourage information security culture within organisations by means of awareness and training. This is also evident from the results of the level of ISP awareness training survey. According to Da Veiga *et al*. (2007), the processes and procedures defined at organisational level, together with the guidance from managers can shape the attitudes of employees. Hence this study also undertook an experimental study to determine the influence ISP awareness training has on end user's attitudes toward ISP compliance

7.4 DESCRIPTIVE ANALYSIS OF THE EXPERIMENTAL QUESTIONNAIRE

The analysis of the experiment answers this research question:

- *How does ISP awareness training influence end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP?*

In order to answer this research question, the three aspects attitudes, self-efficacy and intentions were measured for both the experimental and control group, in order to measure if there was an effect after the intervention. These measures are discussed by groups in the following sections. Just as previously discussed in section 7.3, strongly agree and agree were combined (collapsed) together to measure the level of agreement or disagreement.

7.4.1 Descriptive statistics for the attitude by group

There were five aspects addressing attitudinal aspects. Strongly agree and agree were combined (collapsed) together to determine the level of agreement of the aspects. The aim was to determine the descriptive patterns of the effect on the ISP awareness training intervention. Only proportions in agreement were presented. The results are shown in Table 7-9.

Table 7-9: Level of agreement on aspects of attitudinal by group

Statement	Level of agreement for treatment group			Level of agreement for control group		
	Pre-Agree	Post-Agree	% Change	Pre-Agree	Post-Agree	% Change
ATT1. I feel that compliance to information security policies is a positive thing	92.9% (78)	97.6% (82)	4.7% (4)	100% (89)	96.6% (86)	-3.4% (3)
ATT2. I feel that compliance to information security policies is important	97.6% (82)	96.4% (81)	-1.2% (1)	98.9% (88)	97.8% (87)	-1.1% (1)
ATT3. Following the organisation's ISP is a good idea	92.9% (78)	97.6% (82)	4.7% (4)	97.8% (87)	97.8% (87)	0%
ATT4. Information security policy helps secure computer systems	95.2% (80)	96.4% (81)	-1.2% (1)	97.8% (87)	92.1% (82)	-5.7% (5)
ATT5. Following the organisation's ISP is a necessity	91.7% (77)	97.6% (82)	5.9% (5)	96.6% (86)	94.4% (84)	-2.2% (2)

In terms of the treatment group, the aspects ATT1, ATT3 and ATT5 had an agreement in percentage that increased after the intervention indicating that the intervention might have had a positive effect. Whereas ATT2 aspect resulted in a slight decrease indicating that the ISP awareness training intervention might have had a negative effect.

However for the control group all the aspects had a decrease except the aspect ATT3 which neither increased nor decreased. The results shows that the control group's attitude toward complying with their organisation's ISP did not change when tested the second time around, this can be attributed to the fact that they did not receive the intervention and thus no positive effect could be produced; unlike the treatment group which had a positive change in attitude after the intervention, implying that the change can be attributed to the intervention. Puhakainen (2010) suggests that both security awareness and training interventions seeks to achieve

sustainable attitudinal and behavioural improvements towards policies in end-users. This statement is consistent with the notion that ISP awareness training is an important factor in influencing end-users attitudes toward ISP compliance.

7.4.2 Descriptive Statistics for Self-Efficacy by Group

Strongly agree and agree were collapsed together to determine the aspects were respondent were in agreement. There were seven items measuring self-efficacy and they are shown in Table 7-10.

Table 7-10: Level of agreement on aspects of self-efficacy by group

Statement	Level of agreement for treatment group			Level of agreement for control group		
	Pre-Agree	Post-Agree	% Change	Pre-Agree	Post-Agree	% Change
SEFY1. I have the necessary skills to fulfil the requirements of the ISP	71.9% (64)	88.1% (74)	16.2% (10)	71.9% (64)	68.5% (61)	-3.4% (3)
SEFY2. I have the necessary knowledge to fulfil the requirements of the ISP	70.8% (63)	92.9% (78)	22.1% (15)	70.8% (63)	65.2% (58)	-5.6% (5)
SEFY3. I can use information security measures if I can call for help if I get stuck	71.9% (64)	92.9% (78)	21.0% (16)	71.9% (64)	69.7% (62)	-2.2% (2)
SEFY4. I have the necessary skills to protect myself from information security violations	69.7% (62)	86.9% (73)	17.2% (11)	69.7% (62)	71.9% (64)	2.2% (2)
SEFY5. I have the expertise to implement preventative measures to stop people from getting my confidential information	60.7% (54)	90.5% (82)	29.8% (28)	60.7% (54)	71.9% (64)	11.2% (10)
SEFY6. It is easy for me to enable security features on my work computer by myself	56.2% (50)	88.1% (74)	31.9% (24)	56.2% (50)	68.5% (61)	12.3% (11)
SEFY7. I believe that it is within my control to protect myself from information security violations.	83.1% (74)	94.0% (79)	10.9% (79)	83.1% (74)	82.0% (73)	-1.1% (1)

All the aspects in the treatment group showed an increase in percentage ranging from 10.9% to 31.9%, after the intervention. On the other hand, for the control group all aspects showed a decrease except the aspects SEFY4, SEFY5 and SEFY6. The increase was 2.2%, 11.2 and 13.3%, respectively. These findings suggest that end-

users believed more that they are capable of complying with their organisation's ISP after the intervention in the treatment group. This is consistent with Ajzen's (2002) theory of planned behaviour, implying that controlled beliefs which are concerned with the presence of factors such as required skills and or abilities (in the context of this study ISP awareness training) can facilitate or inhibit performance of behaviour (Ajzen, 1991; McEachan *et al*., 2011).

7.4.3 Descriptive statistics for intention to comply with the ISP by group

There were five aspects addressing intention to comply with the information security policy issues. Strongly agree and agree were collapsed together as discussed earlier to determine the level of agreement and the information is shown in Table 7-11.

Table 7-11: Level of agreement on aspect on intention to comply with the ISP by group

Statement	Level of agreement for treatment group			Level of agreement for control group		
	Pre-Agree	Post-Agree	% Change	Pre-Agree	Post-Agree	% Change
INT1. I intend to comply with information security policies	97.6% (82)	96.4% (81)	-1.2% (1)	92.1% (82)	94.5% (85)	2.4% (3)
INT2. I intend to assist others in complying with information security policies	90.5% (76)	97.6% (82)	7.1% (6)	91.0% (81)	89.9% (80)	-1.1%
INT3. I am likely to follow the organisation's ISP in the future	94.0% (79)	97.6% (82)	3.6% (3)	95.5% (85)	94.4% (84)	-1.1% (1)
INT4. I would follow the organisation's ISP whenever possible	96. 4% (81)	96.4% (81)	0%	96.6% (86)	94.4% (84)	-2.2% (2)
INT5. I am certain I will adhere to my organisation's ISP.	95.2% (80)	97.6% (82)	2.4% (2)	95.5% (85)	92.1% (82)	-3.4% (3)

In terms of the treatment group, the aspects INT2, INT3 and INT5 had increases in the levels of agreement indicating that the intervention might have had a positive effect. The aspect INT1 resulted in a slight decrease indicating that the intervention might have had a negative effect whilst the aspect INT4 showed no difference between the pre-test ratings and the post-test ratings. Overall the results show that end-users had strong intentions to comply with their organisation's ISP after the

intervention. For the control group all the aspects showed a decrease except the aspect “INT1, which had a percentage increase of 2.2%.

The next section discusses the distribution of the continuous variables and presents the paired t-tests and independent-tests. The paired t-test were used to examine the effect of experiment by analysing the difference in mean scores of the pre *and* post-test items of each participant, whilst the independent-tests were used to compare the means of the two-groups (the experimental and control group). Welman *et al*. (2005) accentuates that independent *t-tests* are used to determine whether two-groups have equivalent or different mean scores, and whether an observed difference in the means of the two-groups is sufficiently large to be attributed to a change in some variable or if it could have occurred by chance.

7.5 ANALYSIS OF THE EFFECT OF THE EXPERIMENT

The experimental study consisted of pre *and* post-tests measurements of end-users’ attitude, self-efficacy and intention to comply. The pre *and* post-test measurements are conducted before and after the exposure (awareness and training) to determine whether the exposure had an effect on the end-users’ attitudes toward complying with their organisation’s ISP. According to Welma *et al*. (2005), data analysis by means of statistical techniques helps to investigate variables as well as their effect. Therefore the data collected for the experiment to determine whether awareness training influenced end-users’ attitudes toward complying with their organisation’s ISP will be analysed using dependent *matched-paired t-test.*

T-tests are parametric techniques used for dependent or independent samples (Corder and Foreman 2014), which require assumptions about the variance between the groups, i.e. when we use different participants the assumption is basically that there is variance in any other experimental condition (Field and Hole, 2002). Furthermore, the assumption about the parametric tests is that the sample should be large enough and appropriately resemble a normal distribution (Corder and Foreman, 2014). In this case the observations were randomly selected and normality was achieved by applying the central limit theorem. According to Levine *et al.* (2016), the central limit theorem states that “as the sample size (the number of values in each sample) gets large enough, the sampling distribution of the mean is

approximately normally distributed. This is true regardless of the shape of the distribution of the individual values in the population," Since the sample size was 173, the normality was achieved by using the central limit theorem.

According to Groebner *et al*. (2011) and Levine, Krehbiel and Berenson (2013), paired samples or dependent samples are selected in such a way that values in one sample are matched with the values in the second sample for the purpose of controlling for extraneous factors. The paired samples in this case were the pre-test *and* post-test where two measurements were taken from one person. The differences of the scores between the two tests were assumed to be randomly and independently assigned to groups selected (Leary, 2012; Welman *et al*., 2005).

In this case the aim was to determine whether there were any differences before introducing the experiment. The paired t-test was used to determine whether the rating in the pre-test was not different from that of the post-test in terms of attitudinal, self-efficacy and intention to comply. The results are discussed in the following sections. The p-value approach was used at the 5% level of significance. A p-value less than .05 would lead to the rejection of the null hypothesis of equal means.

7.5.1 Paired t-test to determine difference of pre *and* post-test scores

Firstly, the paired t-tests were done by determining the difference between pre-tests *and* post-tests. If the end-users gave the same ratings we would expect the mean difference to be zero. The researcher first did a one–sample t-test to determine whether the difference is zero which is equivalent to the paired t-tests. The test was done to determine whether the differences had an average of zero. The results of the t-test are discussed in the following sections.

Attitudinal Analysis

All aspects had p-values greater than .05 and thus the null hypothesis that the differences were zero was not rejected. Therefore there was no difference between the pre-test rating and the post-test rating in terms of attitudinal issues. In other words the ISP awareness training did not significantly improve the end-users attitudes toward complying with the ISP. These results imply that ISP awareness training may not directly influence attitudes.

Self-efficacy

All aspects had p-values less than .05 except the aspects "*SEFY1_GAP: I have the necessary skills to fulfil the requirements of the ISP*"; "*SEFY3_GAP: I can use information security measures if I can call for help if I get stuck*" and "*SEFY7_GAP: I believe that it is within my control to protect myself from information security violations*" with p-values greater than .05. The significant tests are shown in Table 7-12.

Table 7-12: One sample t-test of the differences for self-efficacy

Aspects	Test value = 0			95% Confidence Interval of the Difference	
	t-value	p-value	Mean diff	Lower	Upper
SEFY2_GAP. I have the necessary knowledge to fulfil the requirements of the ISP	2.672**	.008	.2081	.0544	.3618
SEFY4_GAP. I have the necessary skills to protect myself from information security violations	2.816**	.005	.2081	.0622	.3540
SEFY5_GAP. I have the expertise to implement preventative measures to stop people from getting my confidential information	3.799**	.000	.2775	.1333	.4216
SEFY6_GAP. It is easy for me to enable security features on my work computer by myself.	4.905**	.000	.3757	.2245	.5269
SEFY_GAP. Self-efficacy gap	3.595**	.000	.2015	.0909	.3121
* p < .05 and ** p < .01					

The dimension self-efficacy showed that there was a difference in four of the aspects and also the overall composite variable. The rating of pre-test *and* post-test differed on the aspects:

- SEFY2_GAP. I have the necessary knowledge to fulfil the requirements of the ISP
- SEFY4_GAP. I have the necessary skills to protect myself from information security violations
- SEFY5_GAP. I have the expertise to implement preventative measures to stop people from getting my confidential information

- SEFY6_GAP. It is easy for me to enable security features on my work computer by myself
- SEFY_GAP. Self-efficacy gap

The mean differences were .2081, .2081, .1333, .2245 and .0909, respectively. Thus the post-test rating was more than the pre-testing. All tests were highly significant. Since most of the aspects of the dimension self-efficacy had mean ratings of pre-testing differing form mean ratings of post-test, it can be inferred that awareness training had a positive impact on self-efficacy.

Intention to comply

All aspects had p-values greater than .05 and thus the null hypothesis that the differences were zero was not rejected. Thus it can be concluded that there was no difference between the pre-test rating and the post-test rating in terms of intention to comply with organisation's ISP.

7.5.2 Paired t-test to determine the difference of the pre *and* post-test by groups.

In this case the researcher wanted to find out the effect of the intervention. The main aim was to determine whether they differed by group by looking at the dimensions.

Difference of at titudinal aspects by group

Out of the four aspects, the aspect, "*ATT2_GAP: I feel that compliance to information security policies is important*" had a p-value greater than .05 indicating that the intervention did not have an effect. However the other aspects were significant as shown in Table 7-13.

Table 7-13: T-tests to determine mean difference of attitudinal aspects by group

Variable	Group	Mean diff	T-test	p-value	Decision
ATT1_GAP. I feel that compliance to information security policies is a positive thing.	Treatment	.2024	2.062*	.041	*The null hypothesis is rejected*
	Control	-.0449			
ATT3_GAP. Following the organisation's ISP is a good idea.	Treatment	.2143	2.943**	.004	*The null hypothesis is rejected*
	Control	-.1124			
ATT4_GAP. Information security policy helps secure computer systems	Treatment	.1786	3.470**	.001	*The null hypothesis is rejected*
	Control	-.2247			
ATT5_GAP. Following the organisation's ISP is a necessity.	Treatment	.1429	3.311*	.022	*The null hypothesis is rejected*
	Control	-.1348			
ATT_GAP. Attitudinal gap	Treatment	.1571	2.833**	.005	*The null hypothesis is rejected*
	Control	-.1124			
* p < .05 and ** p < .01					

The aspect "*ATT1_GAP: I feel that compliance to information security policies is a positive thing.*" mean differences for treatment and control were .2024 and -.0049, respectively. The t-value was 2.062 with a p-value of .041, which is less than .05. This shows that there is a difference between the pre-test *and* post-test as depicted by the confidence interval error bar in Figure 7-3.

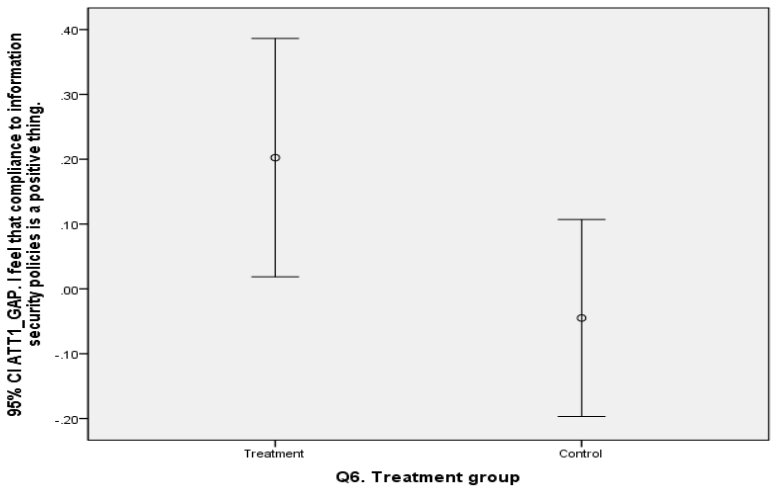


Figure 7-3: Confidence interval error bar showing mean differences of the aspect ATT1_GAP by group.

There was not much overlap between the two-groups indicating the larger mean difference between pre-test *and* post-test was obtained from the treatment group.

Thus the intervention had a positive effect when it comes to compliance to information security policies being a positive thing.

In terms of the aspect, "*ATT3_GAP, following the organisation's ISP is a good idea" the* mean differences for control was -.0449, whilst that for the treatment group was .0476. The confidence interval error bars are shown in Figure 7-4.

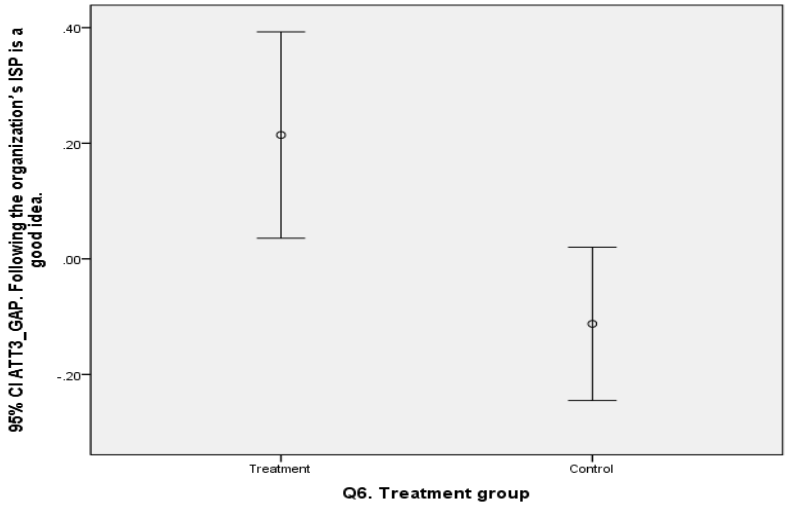


Figure 7-4: Confidence interval error bar showing mean difference of the aspect ATT3_GAP by group

There was no overlap between the two-groups indicating that the intervention had a positive effect. Thus the participants were now of the opinion that following the organisation's ISP is a good idea.

The same pattern was also depicted from the aspect "*ATT4_GAP: Information security policy helps secure computer systems*" where mean differences for control was -.2247 whilst that for treatment was -.2247. The t-value was 3.470 with a p-value of .001. It was highly significant. It is also evidenced in the confidence interval error bar in Figure 7-5.

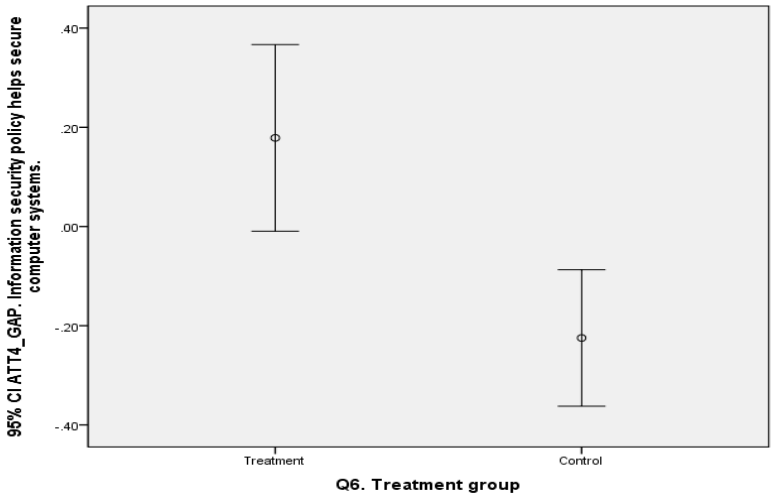


Figure 7-5: Confidence interval error bar showing mean difference of the aspect ATT4_GAP by group

There was no overlap between the two groups, thus after the intervention the participants were more in agreement that information security policy helps secure computer systems.

The aspect "*ATT5_GAP: Following the organisation's ISP is a necessity*" had a t-value of 3.311 with a p-value of .022 leading to the rejection of equal means. The mean difference for control was -.1348 whilst that for treatment was -.1429.The confidence interval error bar is shown in Figure 7-6.

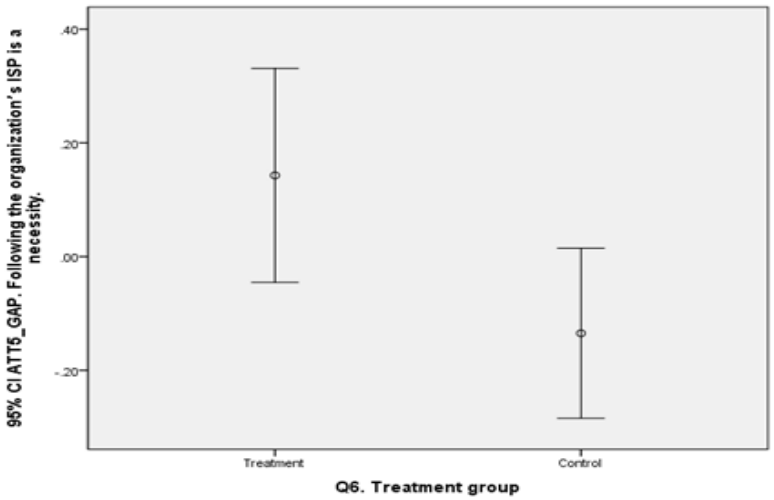


Figure 7-6: Confidence interval error showing mean differences of the aspect ATT5_GAP

Overall the mean differences for the attitudinal dimension were -.1124 and .1571 for the control and treatment groups, respectively. The confidence interval error bars are shown in Figure 7-7.

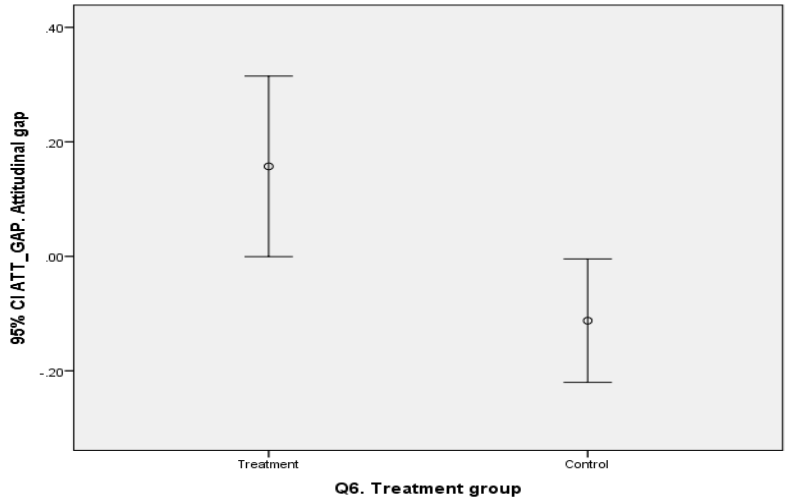


Figure 7-7: Confidence interval error bar showing mean difference of the dimension attitudinal by group

There was no overlap between the two groups, indicating that the intervention resulted in participants rating attitudinal aspects higher. The treatment group had significantly higher rankings than the control group. Thus the intervention had a positive effect when it comes to following the organisation's ISP is a necessity.

Difference of self-efficacy aspects by group

There were 7 aspects measuring efficacy and a composite variable which was calculated by obtaining the mean of the seven variables. The aspects *"I have the necessary skills to fulfil the requirements of the ISP", "I have the necessary skills to protect myself from information security violations"* and *"I have the expertise to implement preventative measures to stop people from getting my confidential information"* had p-values greater than .05 indicating that there was no difference between pre-rating *and* post-rating. The aspects that were significant are shown in Table 7-14.

Table 7-14: T-tests to determine mean difference of self-efficacy aspects by group

Variable	Group	Mean diff	T-test	p-value	Decision
SEFY2_GAP. I have the necessary knowledge to fulfil the requirements of the ISP	Treatment	.4643	3.283**	.001	*The null hypothesis is rejected*
	Control	-.0337			
SEFY3_GAP. I can use information security measures if I can call for help if I get stuck	Treatment	.3571	2.928**	.004	*The null hypothesis is rejected*
	Control	-.0787			
SEFY6_GAP. It is easy for me to enable security features on my work computer by myself	Treatment	.5357	2.048*	.042	*The null hypothesis is rejected*
	Control	2247			
SEFY7_GAP. I believe that it is within my control to protect myself from information security violations	Treatment	.2500	2.399*	.018	*The null hypothesis is rejected*
	Control	-.0674			
SEFY_GAP. Self-efficacy gap	Treatment	.3588	2.781**	.006	*The null hypothesis is rejected*
	Control	.0530			
* p < .05 and ** p < .01					

In terms of the aspect, SEFY2_GAP: "*I have the necessary knowledge to fulfil the requirements of the ISP*", the mean differences for treatment and control were .4643 and -.0337, respectively. The t-value was 3.283 with a p-value of .001 which is less than .05. It was highly significant. Thus there was a difference in the pre-test *and* post-test as depicted by the confidence interval error bar in Figure 7-8

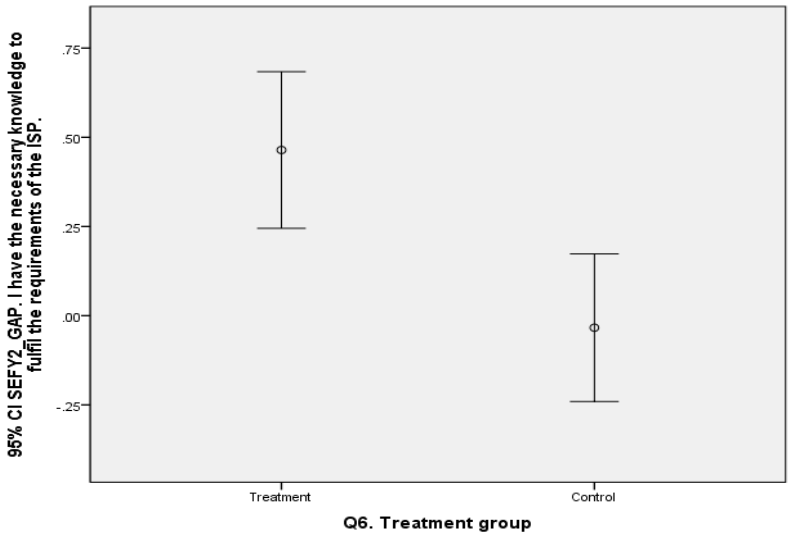


Figure 7-8: Confidence interval error bar showing mean differences of SEFY2_GAP

There was no overlap between the treatment and control groups. The treatment group had significantly higher rankings than the control group. Thus the intervention had a positive effect when it comes to having the necessary knowledge to fulfil the requirements of the ISP.

For the aspect, "*I can use information security measures if I can call for help if I get stuck" t*he test gave a t-value of 2.928 with a p-value of .004, leading to the rejection of the null hypothesis of having a mean difference of zero. The mean difference for control was -.0787, whilst that for the treatment group was .3571. The confidence interval error bars are shown in Figure 7-9.

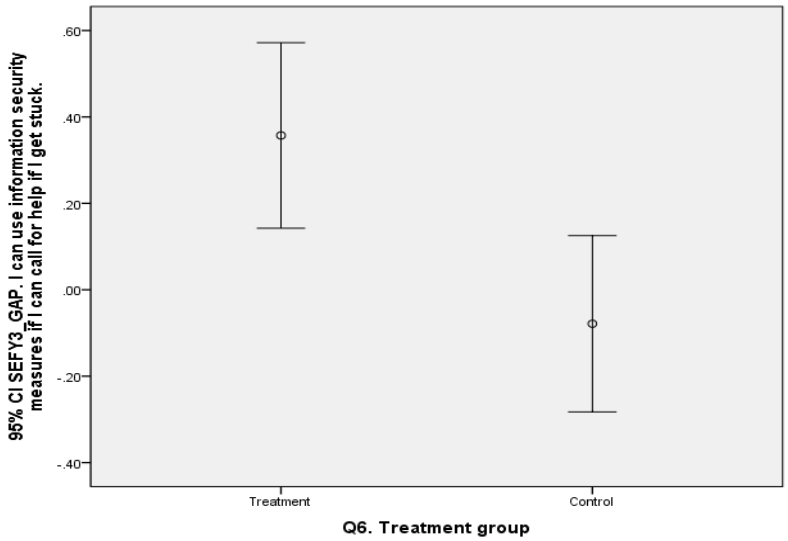


Figure 7-9: Confidence interval error bar showing mean difference of SEFY3_GAP

There was no overlap between the two groups, indicating that the intervention had a positive effect. Thus the participants were of the opinion that they can use information security measures if they can call for help when they get stuck.

The aspect "*It is easy for me to enable security features on my work computer by myself*" had mean differences of .5357 and .2247 for treatment and control, respectively. The t-value was 2.048 with a p-value of .042. Since .042 was less than .05 the null hypothesis of mean difference being zero was rejected. The treatment group had higher ratings that the control group. The confidence interval error bars are shown in Figure 7-10.

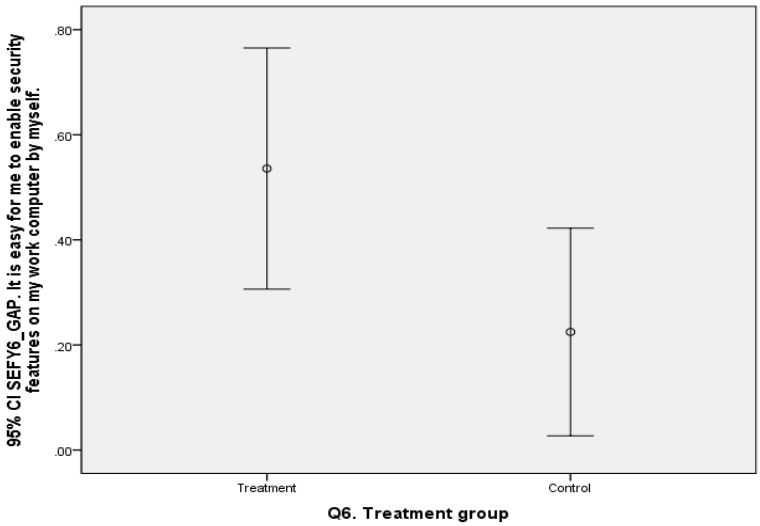


Figure 7-10: Confidence interval error bar showing mean difference of SEFY6_GAP

There was not much overlap between the treatment and control group. The treatment group had higher mean difference indicating that the post-test ratings were higher than the pre-test ratings, Thus after the intervention the participants were more in agreement that it is easy for them to enable security features on their work computer by themselves.

The aspect "*I believe that it is within my control to protect myself from information security violations*" had a t-value of 2.399 with a p-value of .018 leading to the rejection of the null hypothesis of equal means. The mean difference for control was -.0674 whilst that for treatment was .2500. The confidence interval error bars are shown in Figure 7-11.

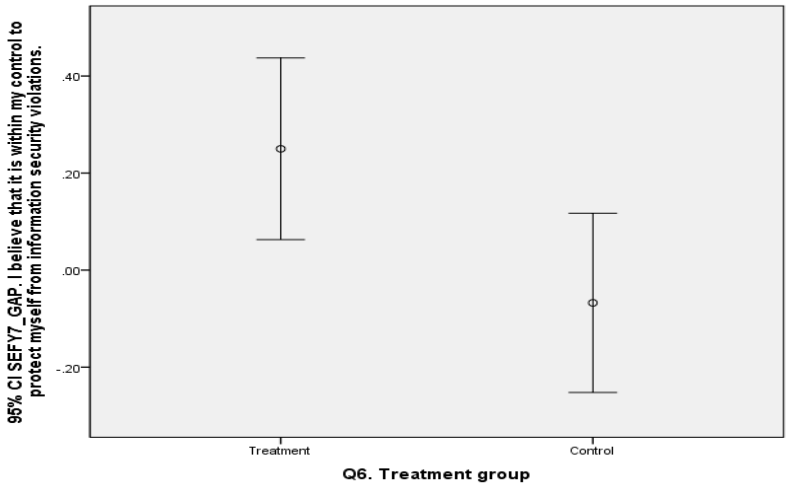


Figure 7-11: Confidence interval error bar showing mean difference of SEFY7_GAP

There was not much overlap between the two groups, indicating the larger mean difference between pre-test *and* post-test was obtained from the treatment group. The participants increased their ratings on the aspect that they believe that it is within their control to protect themselves from information security violations.

Overall the mean differences for the self-efficacy dimension were .3588 and .0530 for control and treatment groups, respectively. The confidence interval error bar is shown in Figure 7-12.

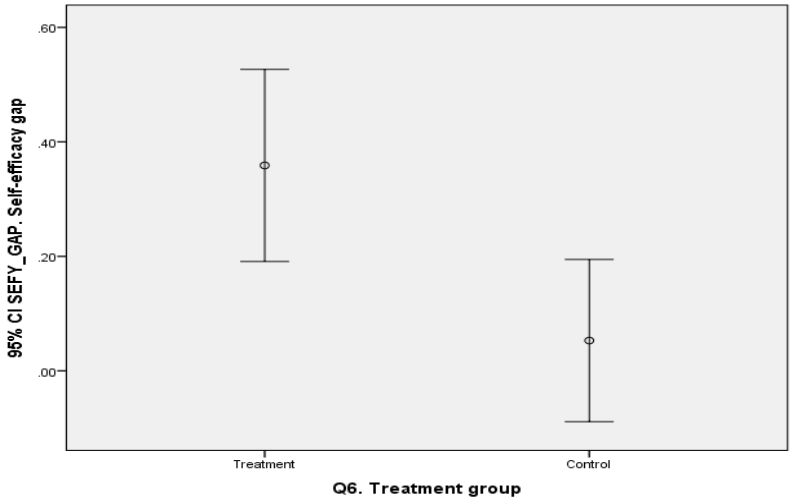


Figure 7-12: Confidence interval error bar showing mean difference of the dimension self-efficacy by group

There was no overlap between the two groups, indicating that the intervention resulted in participants rating self-efficacy aspects higher.

Difference of intention to comply by group

All aspects had p-values greater than .05, thus leading to the non-rejection of the hypothesis of equal means. Thus the intervention did not change the ratings of the aspects on intention to comply.

In addition ANOVA tests were done to determine if there were any significant differences among the three locations. The results of the ANOVA are presented and discussed in the following section.

7.6 ANALYSIS OF THE MEAN DIFFERENCE OF PRE-POST TEST SCORES BY LOCATION

According to Heavey (2014), analysis of variance (ANOVA) is the test that is used when comparing the means from a single dependent variable among two or more groups. Thus the one-way ANOVA was used to test whether the mean difference were the same for the three locations.

Moreover, there are three assumptions that must be met before ANOVA is used. The assumptions are that the observations should be independent, normally distributed and that the variance of the groups should be equal (homogeneity of variance). The assumption of independence was met because the participants were randomly assigned to groups and the central limit theorem was used to assume that the mean differences between the pre-test scores and post-test were approximately normally distributed since the data set was large (greater than 30). According to Johnson and Kuby (2012) and Heavey (2014), the central limit theorem states that the sampling distribution of sample means will more closely resemble the normal distribution as the sample size increases. Furthermore, the assumption of homogeneity of variance was tested. If the ANOVA was significant, post hoc analysis were done to determine the differences. Where the assumption was met the Tukey B was used for the post hoc analysis and where it was violated the post-hoc analysis was done using the Games-Howell test to determine where the differences really existed. The Games-Howell test (GH test) is designed for unequal variances and unequal sample sizes (De Muth, 2014). According to De Muth (2014), the Games-Howell test is a pairwise procedure based on the q-distribution and is an extension of the Tukey-Kramer test and is recommended when sample sizes are greater than five. This test will be used to test for the differences in means when assumption of homogeneity of variance is violated.

The analysis of variance was used to determine whether the mean differences exist between the locations Mafikeng, Potchefstroom and Zeerust. The confidence interval error bars were used to determine where the difference lies diagrammatically. Overlapping of the bars shows that groups are the same whilst the groups that have bars that do not overlap means that there are statistically significantly different from each other. The null hypothesis to be tested was:

- **H_o:** The means differences are equal
- **H_1:** At least one of the pairs of mean difference is different

The test was done at the 5% level of significance. Rejection of the null hypothesis implies that at least one pair of mean difference is different. Only variables with significant mean differences will be presented.

7.6.1 ANOVA test to determine the mean difference of attitudinal by location

The mean differences between pre-test rating *and* post-test ratings were calculated and used to determine whether the attitudinal aspects differed by location. All p-values were greater than .05 and thus the null hypothesis was not rejected. Thus the rating for pre-testing and those for post-testing were the same for the locations. One can conclude that there was homogeneity in terms of the mean differences across locations. In other words, there is no significant attitudinal difference among the end-users of the three locations.

7.6.2 ANOVA test to determine the mean difference of self-efficacy by location

In terms of the dimension self-efficacy, all p-values were greater than .05 except for the aspects "*I have the necessary skills to fulfil the requirements of the ISP*", "*I have the expertise to implement preventative measures to stop people from getting my confidential information*", "*I believe that it is within my control to protect myself from information security violations*" and the overall dimension of self-efficacy which had p-values of .007, .030, .023 and .006, respectively. The information is shown in Table 7-15.

Table 7-15: ANOVA test for the difference between mean difference of the dimension self-efficacy by location

Aspect	Group	Mean	F-square Value	p-value	Decision
SEFY2_GAP. I have the necessary knowledge to fulfil the requirements of the ISP.	Mafikeng	.1053	5.183**	.007	Reject the null hypothesis
	Potchefstroom	.3361			
	Zeerust	-.5000			
SEFY5_GAP. I have the expertise to implement preventative measures to stop people from getting my confidential information.	Mafikeng	.2632	3.580*	.030	Reject the null hypothesis
	Potchefstroom	.3613			
	Zeerust	-.3125			
SEFY7_GAP. I believe that it is within my control to protect myself from information security violations.	Mafikeng	.0000	3.875*	.023	Reject the null hypothesis
	Potchefstroom	.1849			
	Zeerust	-.4375			
SEFY_GAP. Self-efficacy gap	Mafikeng	.1241	5.317**	.006	Reject the null hypothesis
	Potchefstroom	.2953			
	Zeerust	-.3125			
* *p<.05 and* ** *p<.01*					

In terms of the dimension "*I have the necessary skills to fulfil the requirements of the ISP*", the F-value was 5.183 with a p-value of .007. Thus, the null hypothesis of equal means was rejected on the aspect. The test of homogeneity of variance gave a p-value of .001, indicating that the variances among groups were different. The Games-Howell post hoc analysis was used and it gave two homogeneous groups shown in Table 7-16.

Table 7-16: Homogeneous groups for the aspect "I have the necessary knowledge to fulfil the requirements of the ISP" by location

		Group	
Q5. Location of work area	**N**	1	2
Zeerust	16	-.5000	
Mafikeng	38	.1053	.1053
Potchefstroom	119		.3361

The lowest mean of -.5000 was for Zeerust, while the highest mean of .3361 was for Potchefstroom. The participants from Zeerust had lower ratings in the post-test than in the pre-test. The other locations had positive mean differences indicating that the post-test ratings were higher than the pretesting ratings. The major difference was

between Zeerust and Potchefstroom as evidenced by non-overlapping of error bars in Figure 7-13.

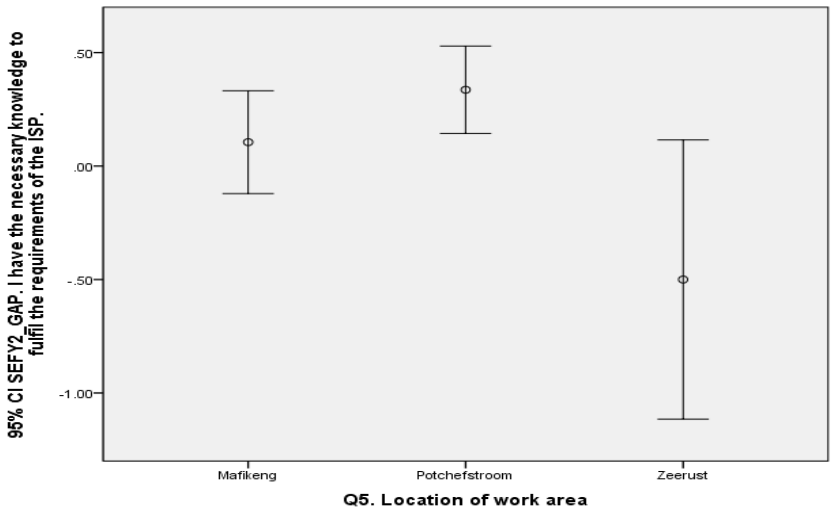


Figure 7-13: Confidence interval error bar of the mean difference ratings for SEFY2_GAP by location

There is no overlap between Zeerust and Potchefstroom. The post- test had higher ratings on Potchefstroom and Mafikeng suggesting that the participants were more in agreement in the post-test on the aspect that they have the necessary skills to fulfil the requirements of ISP.

In terms of the variable "*I have the expertise to implement preventative measures to stop people from getting my confidential information*" the ANOVA test gave a F-value of 3.580 with a p-value = .030, leading to the rejection of the null hypothesis of equal mean differences. The test of homogeneity of variance gave a p-value of .076 indicating that the variances were equal. The Tukey B post-hoc analysis resulted in two groups as indicated in Table 7-17.

Table 7-17: Homogeneous groups for aspect "I have the expertise to implement preventative measures to stop people from getting my confidential information" by location

Tukey B[a,b]			
		Subset for alpha = 0.05	
Q5. Location of work area	N	1	2
Zeerust	16	-.3125	
Mafikeng	38		.2632
Potchefstroom	119		.3613

The same pattern as before was observed where Zeerust had the lowest mean difference of -.3125, while Potchefstroom had the highest mean difference of .3613. Those in Zeerust had higher mean ratings in pre-test than post-test. In Mafikeng and Potchefstroom the post-test ratings were higher than the pre-testing. Zeerust was significantly different from the other groups as shown in Figure 7-14.

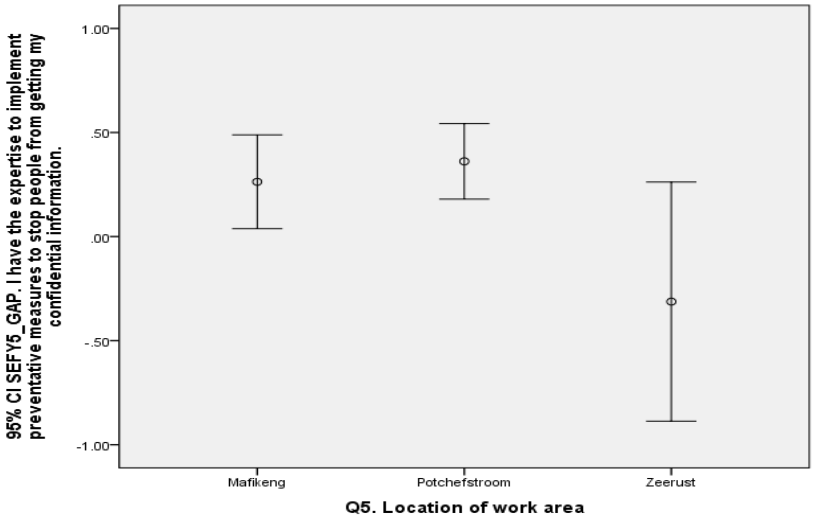


Figure 7-14: Confidence interval error bar of mean difference ratings for SEFY5_GAP by location

There is no overlap between Zeerust and the other locations. The participants from Mafikeng and Potchefstroom were more in agreement on the aspect of having the expertise measures to stop people from getting confidential information in the second test that they had in the pre-test.

The aspect "*I believe that it is within my control to protect myself from information security violations*", had a p-value of .023. Thus, the null hypothesis of equal means was rejected. The test of homogeneity of variance was violated as evidenced by a p-value of .021, indicating the differences of the variances among groups. The Games-Howell post hoc analysis was used and it gave only one homogeneous group as shown in Table 7-18.

Table 7-18: Homogeneous groups for the aspect "I believe that it is within my control to protect myself from information security violations" by location

Q5. Location of work area	N	Group 1
Zeerust	16	-.4375
Mafikeng	38	.0000
Potchefstroom	119	.1849

The lowest mean of -.4375 was for Zeerust, while the highest mean of .1849 was for Potchefstroom. Thus the participants from Zeerust had lower ratings in the post-test than in the pre-test. The other locations had positive mean differences indicating that the post-test ratings were higher than the pretesting ratings. The confidence interval error bars are shown in Figure 7-15.

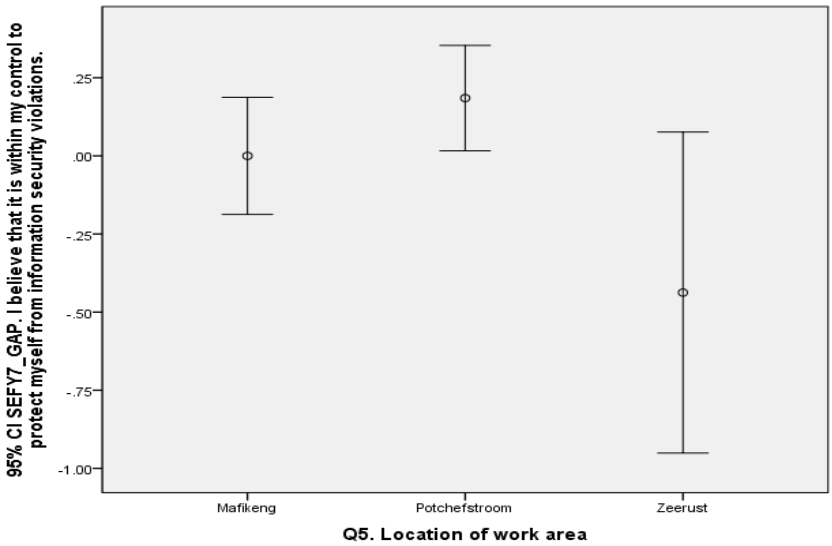


Figure 7-15: Confidence interval error bar of mean difference ratings for SEFY7_GAP by location

There is no overlap between Zeerust and Potchefstroom. The post-test had higher ratings on Potchefstroom. Thus the participants were more in agreement on the post-test on the aspect that they believe that it is within their control to protect themselves from information security violations.

The dimension self-efficacy had an F-value of 5.317 with a p-value of .006 leading to the rejection of the null hypothesis of equal mean differences. The test of homogeneity of variance gave a p-value of .006, indicating that the variances were

not equal. The Games-Howell post-hoc analysis resulted in two-groups as indicated in Table 7-19.

Table 7-19: Homogeneous groups for the dimension self-efficacy by location

Q5. Location of work area	N	Subset for alpha = 0.05	
		1	2
Zeerust	16	-.3125	
Mafikeng	38	.1241	.1241
Potchefstroom	119		.2953

As observed before, Zeerust had the lowest mean difference of -.3125, while Potchefstroom had the highest mean difference of .2953. Those in Zeerust had higher mean ratings in pre-test than post-test. In Mafikeng and Potchefstroom the mean differences were positive, thus the post-test ratings were higher than the pre-testing. The error bars are shown in Figure 7-16.

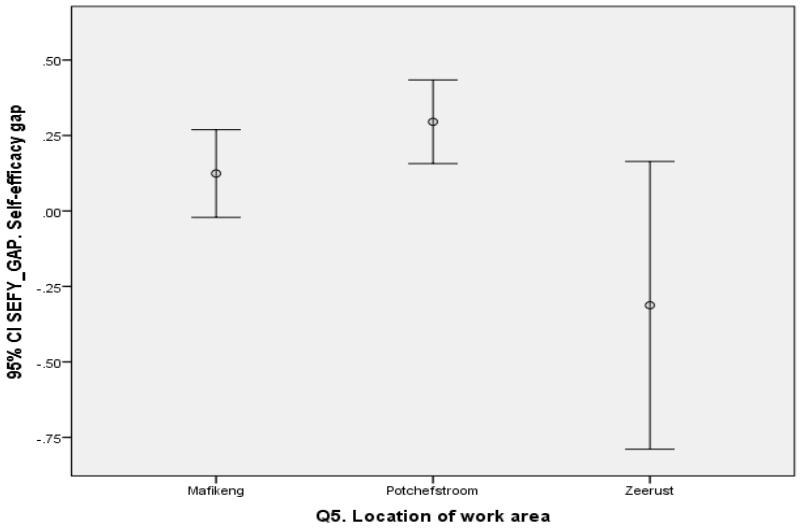


Figure 7-16: Confidence interval error bar of mean difference ratings for the dimension self-efficacy by location

There is no overlap between Zeerust and Potchefstroom. Generally the participants from Mafikeng and Potchefstroom were more in agreement with the issues on self–efficacy in the post- test than they had been in the pre-test. In other words, end-users' self-efficacy about complying with the ISP showed improvement after the ISP awareness training.

7.6.3 ANOVA test to determine the mean difference of intention to comply by location

In terms of the dimension intention to comply, all p-values were greater than .05 except for the aspects "*I intend to assist others in complying with information security policies*" and "*I am likely to follow the organisation's ISP in the future".* The information is shown in Table 7-20.

Table 7-20: ANOVA test for difference between mean difference of the dimension intention to comply

Aspect	Group	Mean	F-square Value	p-value	Decision
INT2_GAP. I intend to assist others in complying with information security policies.	Mafikeng	.0000	3.945*	.021	Reject the null hypothesis
	Potchefstroom	.1681			
	Zeerust	-.3125			
INT3_GAP. I am likely to follow the organisation's ISP in the f0uture	Mafikeng	-.0526	3.167*	.045	Reject the null hypothesis
	Potchefstroom	.1597			
	Zeerust	-.2500			
* *p<.05 and* ** *p<.01*					

The aspect "*I intend to assist others in complying with information security policies*", had mean differences that differed by location as evidenced by an F-value of 3.945 with a p-value of .021. The test of homogeneity of variance gave a p-value of .004, indicating that the variances among groups were different. The Games-Howell post hoc analysis was used and it gave only one homogeneous group as shown in Table 7.21.

Table 7-21: Homogeneous groups for the aspect "I intend to assist others in complying with ISP" by location

Q5. Location of work area	N	Group 1
Zeerust	16	-.3125
Mafikeng	38	.0000
Potchefstroom	119	.1681

The lowest mean of -.3125 was for Zeerust, while the highest mean of .1681 was for Potchefstroom. The participants from Zeerust had lower ratings in the post-test than in the pre-test. In Mafikeng the ratings of the pre-test were the same as the ratings of the post-test. Potchefstroom had positive mean differences indicating that the post-test ratings were higher than the pretesting ratings. The confidence interval error bars are shown in Figure 7.17.

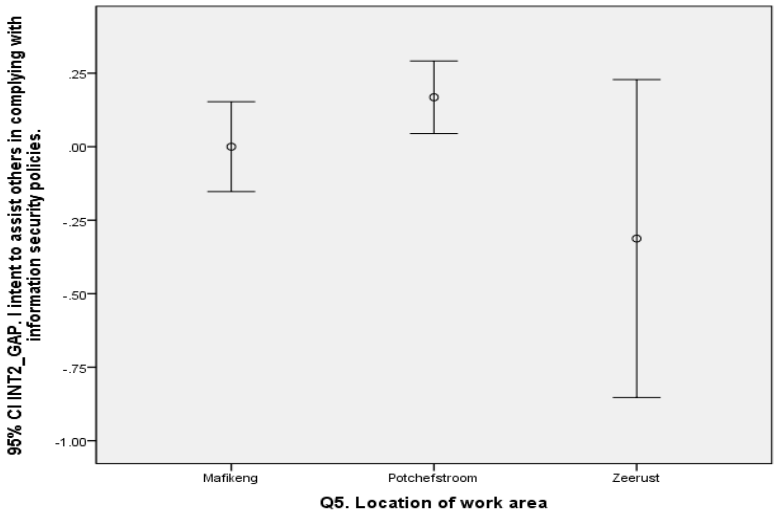


Figure 7-17: Confidence interval error bar of mean difference ratings for INT2_GAP

There is not much overlap between Zeerust and Potchefstroom. The post-test had higher ratings on Potchefstroom suggesting that the participants were more in agreement in the post-test on the aspect of their intention to assist others in complying with information security policies. However, for Zeerust the participants' agreement level decreased in the post-test, implying that the intervention may have not improved participants' intention to assist others in complying with information security policies.

The aspect "*I am likely to follow the organisation's ISP in the future*", had mean differences that differed by location as evidenced by an F-value of 3.167 with a p-value of .045. The test of homogeneity of variance gave a p-value of .075, indicating equality of variance among groups. The Tukey B post hoc test gave result to one homogeneous group as shown in Table 7-22.

Table 7-22: Homogeneous groups for the aspect "I am likely to follow the organisation's ISP in the future" by location

Tukey B[a,b]		
		Subset for alpha = 0.05
Q5. Location of work area	N	1
Zeerust	16	-.2500
Mafikeng	38	-.0526
Potchefstroom	119	.1597

As observed before, the lowest mean of -.2500 was for Zeerust, while the highest mean of .1597 was for Potchefstroom. The participants from Zeerust and Mafikeng had lower ratings in the post-test than in the pre-test. Potchefstroom had positive mean differences indicating that the post-test ratings were higher than the pretesting ratings. The confidence interval error bars are in Figure 7-18.

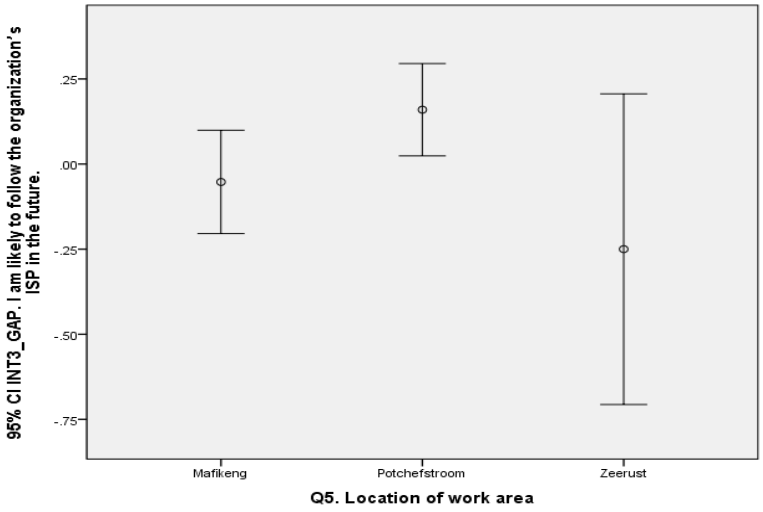


Figure 7-18: Confidence Interval error bar of mean ratings for INT3_GAP

There is some overlap between the groups. The post-test had higher ratings on Potchefstroom, suggesting that the participants were agreed more in the second test, suggesting that they are likely to follow the organisation's ISP in the future. However, for Zeerust and Mafikeng participants, the agreement level decreased in the post-test, implying that the intervention may not have improved the end-users likelihood to follow the organisation's ISP in the future.

7.7 ASSESSMENT OF THE STRUCTURAL MODEL

Structural equation modelling (SEM) is a collection of statistical techniques that allow a set of relationships between one or more independent variables, either continuous or discrete, and one or more dependent variables, either continuous or discrete to be examined (Tabachnick and Fidell, 2014). It is sometimes called path analysis. According to Dugard *et al*. (2010), structural equation modelling (SEM) may combine a measurement model (confirmatory factor analysis) and a structural model (path analysis) to investigate the influence among measured (indicator) variables and latent variables. Thus structural equation modelling consists of two components: a measurement model that relates measured variables to factors and a structural that concerns hypothesised relationships among the constructs (Dugard *et al*., 2010). According to Hair *et al*. (2014), the first stage is using confirmatory factor analysis to provide a confirmatory test for the measurement theory to confirm it, and the second stage is the structural model which is most useful in representing the interrelationships of variables between constructs.

There are several methods that are used to estimate SEM and the maximum likelihood estimator is one of the most common methods. It is a scale free method and an alternative to the ordinary least squares used in multiple regressions. According to Schumacker and Lomax (2010), it assumes multivariate normality of the observed variables (the sufficient conditions are that the observations are independent and identically distributed and that kurtosis is zero). It is a procedure that iteratively improves parameter estimates to minimise a specified fit function (Hair *et al*., 2014). The maximum likelihood estimate is a flexible approach to parameter estimation in which the “most likely” parameter values to achieve the best model fit is found (Hair *et al*., 2014).

The measurement model validity depends on two aspects. Firstly, establishing acceptable levels of goodness of fit for the measurement model, and secondly, finding specific evidence of construct validity. The validity of the measurement is established using a number of measures that determine the goodness of fit of the model. Goodness of fit (GOF) of the model indicates how well the specified model reproduces the observed covariance matrix among the indicator items, that is, the

similarity of the observed and estimated covariance matrices. Some of the goodness of fit measures are:

- Chi-square test
- CFI (Comparative Fit Index)
- RMSEA (Root Mean Square error of approximation)
- RMR (Root Mean Square Residual) and SRMR (Standardised Root Mean Residual)
- IFI (Incremental Fit Index),
- NFI (Normed Fit Index),
- AGFI (Adjusted Goodness of Fit Index)

These various mode fit indices, however, are subjectively interpreted when determining an acceptable model fit (Schumacker and Lomax 2010). According to Hair, *et al*. (2010),

- The Chi-square statistic (χ^2) is the only statistical test of significance included for testing the theoretical model and is the most fundamental goodness of fit test. It ranges from zero when the model is saturated with all paths included to a maximum value for the independent model with no paths included (Schumacker and Lomax 2010). It tests the absolute fit of the model. It is essentially the same as the chi-square test statistics for testing independence between two nonnumeric variables. It is the overall measure of evaluating the overall model and is a measure of difference between the observed and estimated covariance matrices (Hair *et al*., 2014). A chi-square value of zero indicates a perfect fit or no difference between the observed and estimated covariance matrices. The aim of GOF measures is to look for no differences between matrices (low χ^2 values) to support the model as representative of the data. The model fits the data if the p-value is more than .05, that is, the model is non-significant, but it is adversely affected by sample size (Hair et.al. 2014). Thus the need to look at other goodness of fit tests.
- The comparative fit index (CFI) is an incremental fit index that is an improved version of the normed fit index and it is one of the most widely used indices. The comparative fit index (CFI) ranges from 0 to 1 with values close to 1

indicating better fit. CFI values above .90 are usually associated with a model that fits well.

- The Root Mean Square error of approximation (RMSEA) is one of the most widely used measures that attempt to correct for the tendency of the χ^2 goodness of fit (GOF) test statistic to reject models with a larger sample size or large number of observed variables. It better represents how well a model fits the population, not just a sample used for estimation. A lower RMSEA value indicates a better fit. There have been a lot of debates in terms of the cut-off point and previous research has pointed to a cut-off value of .05 or .08. Thus values close to zero indicate a better fit.
- The Root Mean Square Residual (RMR) is the square root of the mean of the squared which means the average of the residual. RMR has a problem that it is related to the scale of the covariance whilst the Standardised Root Mean Residual (SRMR) is not. SRMR represents the average standardised residuals. Lower RMR and SRMR values represent a good fit whilst higher values represent worse fits and this puts RMR, SRMR and RMSEA into a category of indices sometimes known as badness-of-fit measures in which high values are indications of a poor fit. A rule of thumb is that an SRMR over .1 suggests a problem with fit.
- The Goodness of Fit Index is one of the most used indexes. It ranges from 0 to 1 with higher values indicating better fit. Values of GFI above .90 are considered good but others argue that .95 should be used. The adjusted version (AGFI) has a similar interpretation.
- The informed Fit Index TLI), Relative Fit Index (RFI), Incremental Fit Index (IFI), Tucker Lewis Index (TLI)), and many more like IFI (Incremental Fit Index) are expected to be as close as possible to one (and not below .9)
- The criteria of goodness of fit of the other models can be summarised as in Table 7-23.

Table 7-23: Criteria and Acceptable Fit Interpretation

Model-Fit Criterion	Acceptable Level	Interpretation
Chi-square	Tabled χ^2 value	Compares obtained χ^2 value with tabled value for given *df*
Goodness-of-fit index (GFI)	0 (no fit) to 1 (perfect fit)	Value close to .90 or .95 reflect a good fit
Adjusted GFI (AGFI)	0 (no fit) to 1 (perfect fit)	Value adjusted for *df*, with .90 or .95 a good model fit
Root-mean square residual (RMR)	Researcher defines level	Indicates the closeness of Σ to *S* matrices
Standardized RMR (SRMR)	< .05	Value less than .05 indicates a good model fit
Root-mean-square error of approximation (RMSEA)	.05 to .08	Value of .05 to .08 indicate close fit
Tucker–Lewis Index (TLI)	0 (no fit) to 1 (perfect fit)	Value close to .90 or .95 reflect a good fit
Normed fit index (NFI)	0 (no fit) to 1 (perfect fit)	Value close to .90 or .95 reflect a good fit
Parsimony fit index (PNFI)	0 (no fit) to 1 (perfect fit)	Compares values in alternative models
Akaike information criterion (AIC)	0 (perfect fit) to positive value (poor fit)	Compares values in alternative models
Source: Schumacker and Lomax 2010, p76		

According to Hair *et al*. (2014), a researcher should report at least one incremental index and one absolute index in addition to the χ^2 value and the associated degrees of freedom because using a single GOF index, even with a relatively high cut-off value is no better than using the χ^2 GOF test alone. The authors further indicated that one should report the χ^2 and degrees of freedom, the CFI or TLI and the RMSEA, which usually provide sufficient unique information to evaluate a model. The SRMR can be used in place of the RMSEA since they both represent badness of fit. Thus in this case the χ^2, its degrees of freedom, CFI or TLI, and RMSEA or SRMR will be used to determine the goodness of fit of the model.

In this research, structural equation modelling was used to find a model that best describes the phenomena under study as comprehensively as possible and estimates the compatibility of the research model with the collected research data. The confirmatory factor analysis and structural equation modelling will be presented.

7.7.1 Confirmatory factor analysis

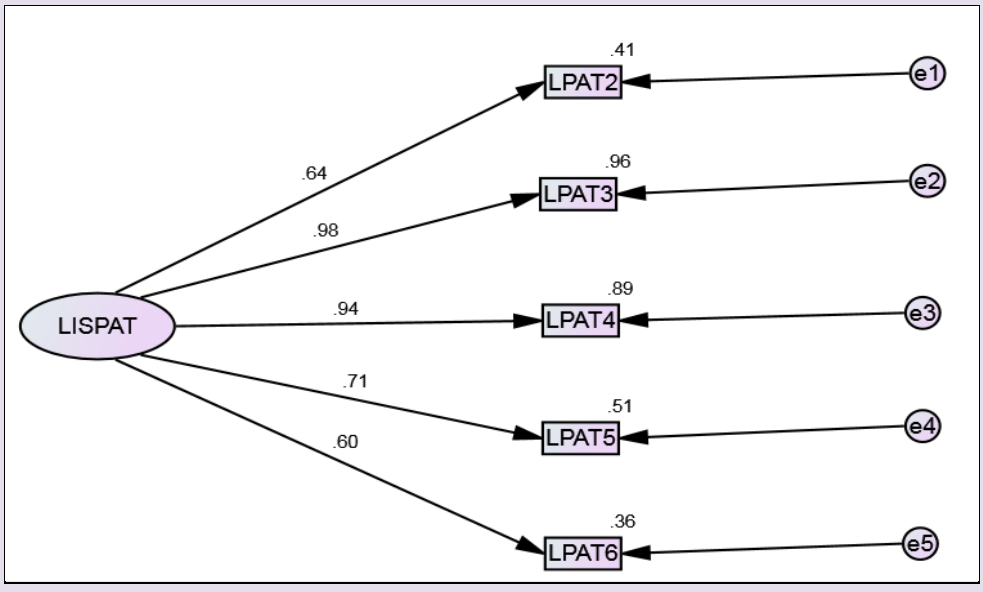
Confirmatory factor analysis (CFA) is a way of testing how well measured variables represent a smaller number of constructs (Hair *et al*., 2014). It is used to study the

relationships between a set of observed variables and a set of continuous latent variables. Thus it is a tool that enables one to either “confirm” or “reject” the preconceived theory.

A confirmatory factor analysis was done to test the relationship between observed variables and underlying variables. This section presents the confirmatory factor analysis of the dimensions. The confirmatory factor analysis was done on the results of the post tests to determine the relationship of ISP awareness training, attitudes, self- efficacy and intention to comply with ISP.

Confirmatory factor analysis on ISP awareness training

The level of ISP awareness training was measured by 7 variables. According to Hair *et al*. (2014), all factor loadings should be statistically significant and a good rule of thumb is that standardised loading estimates should be .5 or higher, and ideally .7 or higher. Thus, in this case, factor loadings of at least .5 were retained. The confirmatory factory factor analysis retained only 5 items as shown in Figure 7-19.



X^2= 3.520, df = 5, p-value = .620; CFI =1,000; GFI=.983; NFI=.988; RFI=.976; IFI=.1.005; TLI=.1.010; RMSEA = .000; RMR = .032; SRMR = .0298

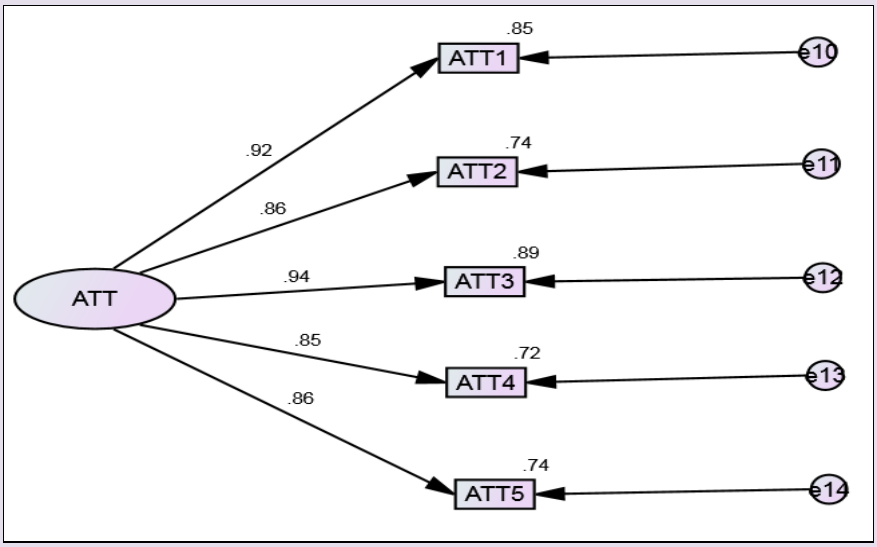
Figure 7-19: Confirmatory factor analysis for ISP awareness training

All factor loadings were above .5. The confirmatory factor analysis (CFA) showed that all model fit indices satisfy the conditions of a good fit. The chi-square value was 3.520 with 5 degrees of freedom. The p-value associated with the result was .620.

Since the p-value is above .05, it is insignificant and thus the χ^2 goodness of fit test showed that there was no significant difference between the observed covariance matrix matched and the estimated covariance matrix within the sample. The value of the CFI (comparative fit index) was 1, whilst GFI (goodness of fit index) was .983 and RMSEA (badness of fit) was .0. The results indicated that the measurement model provided a reasonably good fit.

Confirmatory factor analysis on attitudes

All five factors were retained since all factor loadings were at least .70 as shown in Figure 7-20.



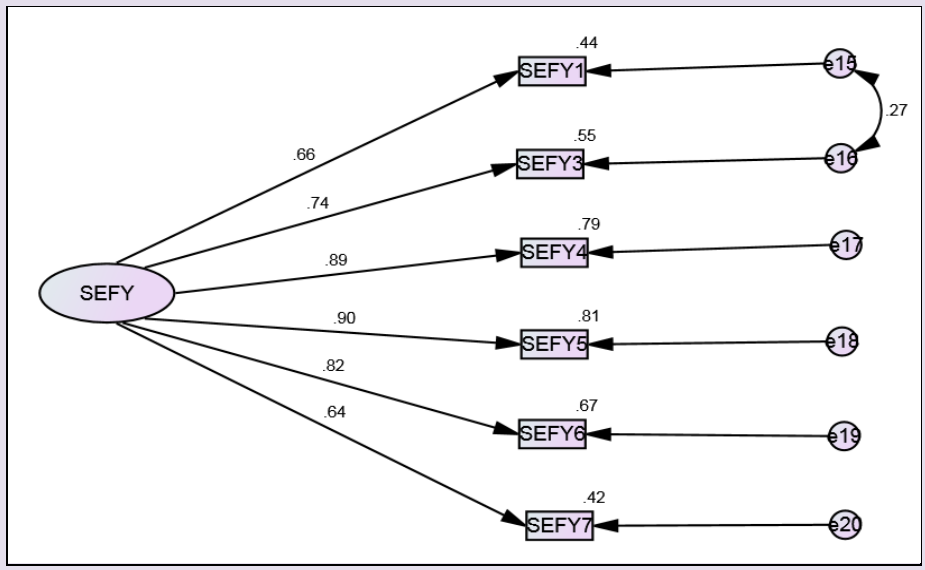
X^2= 9.486, df = 5, p-value = .091; CFI =.989; GFI=.958; NFI=.977; RFI=.955; IFI=.989; TLI=.978; RMSEA = .104; RMR = .008; SRMR = .0185

Figure 7-20: Confirmatory factor analysis on attitudes

The results of the confirmatory factor analysis (CFA) showed that most of the model fit indices satisfy the conditions of a good fit. The chi-square value was insignificant with a value of 9.486, degrees of freedom 2 and a p-value of .091. Thus the χ^2 goodness of fit test showed that there was no significant difference between the observed covariance matrix matched and the estimated covariance matrix within the sample. The value of the indices CFI, GFI and SRMR were .989, .951 and .0185, respectively. Thus the results show that the measurement model provided a reasonably good fit.

Confirmatory factor analysis on self-efficacy

Out of the 7 items, 6 were confirmed to be constructs measuring self-efficacy. All factor loadings were above .7 as shown in Figure 7-21.



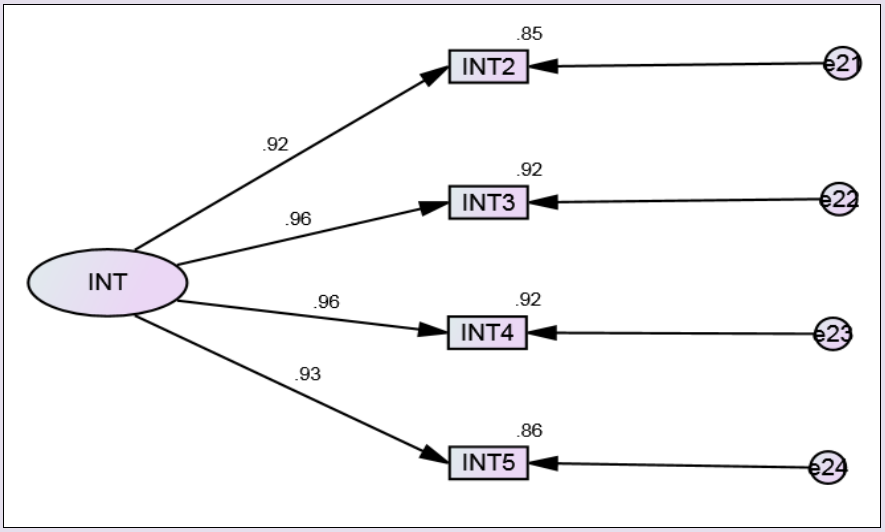
X^2= 8.241, df = 8, p-value = .410; CFI =.999; GFI=.971; NFI=.974; RFI=.951; IFI=.999; TLI=.999; RMSEA = .019; RMR=.014; SRMR = .0234

Figure 7-21: Confirmatory factor analysis on self-efficacy

The chi-square value was 8.241 with an insignificant p-value of .410. The confirmatory factor analysis (CFA) showed that all model fit indices satisfy the conditions of a good fit. The values of CFI, GFI and RMSEA were .999, .971 and .019, respectively. Thus, the results indicated that the measurement model provided a reasonably good fit.

Confirmatory factor analysis on intention to comply with ISP

Out of the 5 items, 4 were confirmed to be the constructs measuring intention to comply with ISP. All factor loadings were above .7 as shown in Figure 7-22.



X^2= .036, df = 2, p-value = .982; CFI=1.000; GFI=1.000; NFI=1.000; RFI=1.000; IFI=1.005; TLI=1.014; RMSEA = .000; RMR=.000; SRMR = .0007

Figure 7-22: Confirmatory factor analysis on intention to comply with ISP

The results of the confirmatory factor analysis (CFA) showed that all of the model fit indices satisfy the conditions of a good fit. The chi-square value was insignificant with a value of .036, degrees of freedom 2 and a p-value of .982. Thus the χ^2 goodness of fit test showed that there was no significant difference between the observed covariance matrix matched and the estimated covariance matrix within the sample. The value of the indices CFI, GFI and RMSEA were 1.000, 1.000 and .000, respectively. Thus the results showed that the measurement model provided a reasonably good fit. SEM was then applied to test the hypotheses. The results are discussed in the following section.

7.8 THE SEM ESTIMATED MODEL

The structural model of the study showed the relationship between ISP awareness training, attitudes, self-efficacy and intention to comply with ISP. The hypotheses tested are indicated below.

7.8.1 Hypotheses to be tested

In order to test the relationship between ISP awareness training, attitudes, self-efficacy and intention to comply with ISP, it is seen fit to reiterate the hypotheses of this study as follows:

Hypothesis 1 (H_1): ISP Awareness training directly influences end-users' attitude to comply with their organisation's ISP

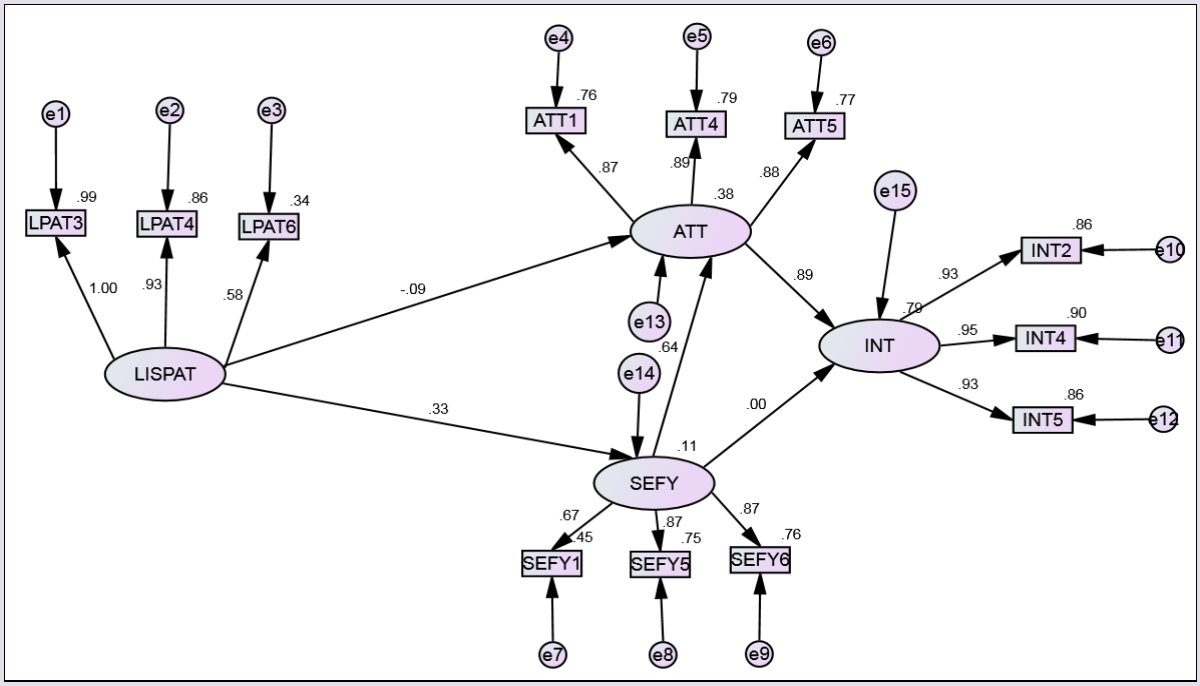
Hypothesis 2 (H_2): ISP Awareness training positively affects end-users' self-efficacy to comply with their organisation's ISP

Hypothesis 3 (H_3): Self-efficacy has a positive influence on end-users' attitudes toward complying with their organisation's ISP

Hypothesis 4 (H_4): Self-efficacy has a positive impact on end-users' intention to comply with their organisation's ISP

Hypothesis 5 (H_5): The end-users' attitude towards complying with their organisation's ISP has a positive impact on their intention to comply

The presentation of the structural part of the model then follows. In order to determine model fitness the researcher used the χ^2, its degrees of freedom, CFI or TLI, and RMSEA or SRMR to determine the goodness of fit of the model. The final SEM model fitted is given in Figure 7-23.



X^2= 62.004, df = 49, p-value = .101; CFI =.985; GFI=.905; NFI=.933; RFI=.910; IFI=.985; TLI=.980; RMSEA = .057; RMR=.042; SRMR=.0550

Figure 7-23: The estimated structural equation model of ISP compliance

One can conclude that the results of the SEM showed that the overall model fit appears to be a good fit as supported by the chi-square with a value of 62.004, with degrees of freedom of 49, and a p-value of .101 indicating that it was insignificant. The value for CFI, the incremental fit index, was .985, while the values for absolute fit indices were .905 for GFI (goodness-of-fit) and.057 for RMSEA (badness-of-fit).Thus the theoretical model presented in Figure 4-2 was used to address the hypotheses of the study.

The multiple regression weights from the model in AMOS are shown in Table 7-24.

Table 7-24: Multiple regression weights for the ISP compliance model

Hypothesis		Estimate	S.E	C,R	P
H_1	ATT←LISPAT	-.051	.056	-.923	.356
H_2	*SEFY←LISPAT*	.248	.087	2.838	.005
H_3	ATT←SEFY	.457	.088	5.183	***
H_4	*INT← SEFY*	.001	..073	.012	.990
H_5	*INT←ATT*	.998	.122	8.180	***
*** means the p-value is less than .001					

Hypothesis 1 (H_1): ISP Awareness training directly affects an employee's attitude to comply with their organisation's ISP.

Looking at the results in Table 7-22, ISP awareness training does not have a significant positive relationship with attitudes. The ***p-value = .356*** and ***β = -.051***. Since the p-value is greater than .05, we do not reject the null hypothesis of no relationship (H_0: ***β=0.)*** and conclude that the parameter is not significantly different from zero (there is no relationship). Thus the hypothesis that ISP awareness training directly affects an employee's attitude to comply with their organisation's ISP is not supported by the data. These results are not in line with similar studies such as Bulgurcu *et al*. (2010), Ifinedo (2012 and 2014), Siponen *et al.* (2014) and Safa *et al*. (2015) who found information security awareness to have a direct effect on attitudes toward ISP compliance.

However, Ajzen (2011) suggests that not all potential outcomes of behaviour are expected to influence attitudes as only beliefs that are readily accessible in memory determine the prevailing attitudes, thus limiting the number of beliefs that provide a basis for an observed attitude toward behaviour. Therefore a rational explanation of

our finding could be that the means used to guide and observe attitudes toward ISP compliance in this study (i.e. the intervention, scale composition, and the research sample), could have had limited direct influence on the readily accessible beliefs prevailing attitudes.

Hypothesis 2 (H_2): ISP Awareness training positively affects an employee's self-efficacy to comply with their organisation's ISP.

The ***p-value =.005*** with ***β = .248***. Since the p-value < .05, we reject the null hypothesis of no relationship at the 5% level of significance. It was highly significant. ISP awareness training significantly impacts positively on end-users' self-efficacy to comply with their organisation's ISP. For every increase of one unit in ISP awareness training, employee's self-efficacy to comply with their organisation's ISP increases by .248. The hypothesis was supported and thus proven true. This finding is in line with Herath and Rao's (2009) findings and suggests that if end-users possess the necessary knowledge and skills, their belief-set about their capability to comply with the ISP (self-efficacy) can be improved.

Hypothesis 3 (H_3): Self-efficacy has a positive influence on end-users' attitudes toward complying with their organisation's ISP.

Figure 7-22 shows that the factor loading between self-efficacy and attitudes was .64, indicating that there was a significant positive relationship between self-efficacy and attitudes. The ***p-value < .001*** with ***β = .457***. Since the p-value < .05, we reject the null hypothesis of no relationship at the 5% level of significance. It was highly significant. Self-efficacy has a positive influence on end-users' attitudes toward complying with their organisation's ISP. For every increase of one unit in self-efficacy, attitudes increases by .457. The hypothesis was supported and thus proven true. Thus high values in self-efficacy are associated with high values in attitudes, suggesting that if users are confident in their ability to comply with their organisation's ISP, their attitudes towards complying with the ISP will also increase to a favourable one. Whilst Sommestad *et al*. (2014) suggest that high values of self-efficacy predicts poor attitude towards compliance, our finding is comparable to Li (2012) and Rezaei, Zamani-Miandashti and Shiraz, 2013), where a positive and significant relationship between attitude and self-efficacy was found.

Hypothesis 4 (H_4): Self-efficacy has a positive impact on end-users' intention to comply with their organisation's ISP.

Looking at Table 7-22, it can be noted that the ***p-value = .990*** with ***β = .001***. Since p-value > .05, we do not reject the null hypothesis of no relationship (H_0: ***β=0.)*** and conclude that the parameter is not significantly different from zero (there is no relationship). The hypothesis that self-efficacy has a positive impact on end-users' intention to comply with their organisation's ISP is not supported by the findings. Similar results were found by Kim *et al*. (2014). However, these findings are not consistent with the tenets of the TPB, which suggest a person needs to have confidence in their capability to carry out a given behaviour, in order to have the intention to perform that behaviour. Similarly, in their studies Bulgurcu *et al*. (2010), Ifinedo (2012 and 2014) and Siponen *et al*. (2014) found self-efficacy to have a positive impact on intentions.

Hypothesis 5 (H_5): The end-users' attitude towards complying with their organisation's ISP has a positive impact on their intention to comply.

Looking at the results in Table 7-22, attitudes have a positive significant relationship with intention to comply with ISP. The ***p-value < .001*** and ***β = .998***. Since the p-value is less than.05 we reject the null hypothesis of no relationship (H_0: ***β=0.)*** and conclude that the parameter is significantly different from zero (there is a relationship). An increase of 1 unit in attitudes is associated by an increase of .998 in intention to comply with ISP. Thus the hypothesis that the end-users' attitude towards complying with their organisation's ISP has a positive impact on their intention to comply is supported by the findings. We can therefore say that the more positive the end-user's attitude is toward ISP compliance, the higher their intention to comply with their organisation's ISP will be. These results are in line with the findings of other studies based on the TPB, were attitudes were found to have a positive effect on intentions (Ifinedo, 2012 and 2014; Kim *et al*., 2014; Safa *et al*., 2016). Moreover, these findings are in line with Tipton and Krause's (2011) proposition of attitudes being targets of change, suggesting that if you can subtly or directly change someone's attitude, you can consequently change their behaviour, as it is often easier to change behaviour through an attitude shift than to change behaviour directly. Likewise, Ajzen (1991) suggests that intentions to perform behaviour can be

predicted with high accuracy from attitudes toward a given behaviour. The model supported by the data is given in Figure 7-24.

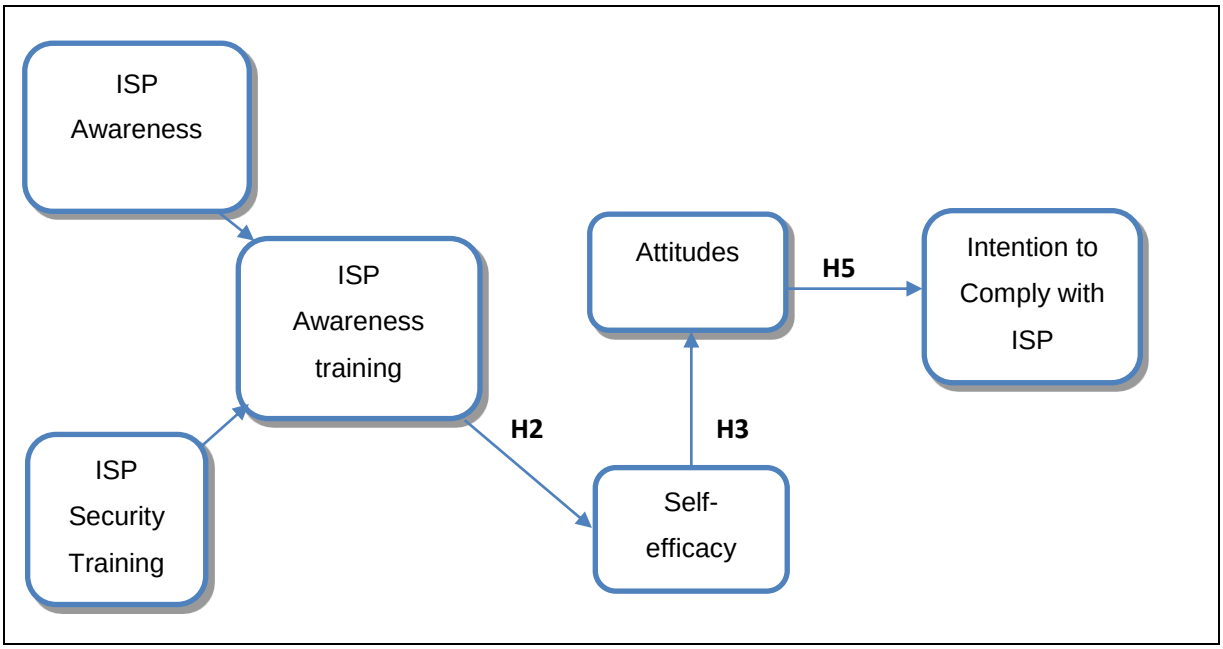


Figure 7-24: The Final ISP compliance model as supported by the findings

The primary objective of this study was to assess the significance of ISP awareness training in influencing end-user attitudes towards complying with their organisation's ISP. The following research question was posited to illustrate this significance.

- *How does ISP awareness training influence end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP?*

The findings regarding the direct relationship of ISP awareness training and attitudes were found to be insignificant. However a significant relationship between ISP awareness and self-efficacy as well as between self-efficacy and attitude was found, indicating an indirect relationship of ISP awareness training and attitudes through self-efficacy. Therefore it is established that if users believe that they are capable of executing the actions required by their organisation's ISP, they are likely to exert a positive response (attitude) towards complying with the ISP.

Furthermore, as presented in the findings, a positive relationship was found to be significant between attitudes and intention, signifying that when users have a positive attitude toward a given behaviour their intention to comply will also increase. Thus

ISP awareness training is found to positively influence end-users' attitude toward ISP compliance. Table 7-25 presents the summary of the research findings.

Table 7-25: Summary of the findings

Number	Hypothesized Path	Results
H_1	ATT←LISPAT	Not Supported
H_2	*SEFY←LISPAT*	Supported
H_3	ATT←SEFY	Supported
H_4	*INT← SEFY*	Not Supported
H_5	*INT←ATT*	Supported

7.9 SUMMARY

This chapter presented the results of the study as well as the analysis and interpretation, with reference to the literature where feasible. The results of the survey as well as the analysis of the experiment findings were discussed in this chapter. Furthermore, all the questions presented in the questionnaire were linked to the research objective of this study.

The questionnaire used in the survey assessed the current level of ISP awareness training and compliance behaviour of the target organisation, whilst the questionnaire used to assess the influence of ISP awareness training on end users' attitudes toward ISP compliance measured the TPB's viability.

Based on the findings presented in this chapter, it is safe to conclude that ISP awareness training intervention does not significantly influence end-users attitudes towards ISP compliance. However a significant impact was observed on end-users' self-efficacy, which in turn had an influence on end-users' attitudes toward complying with their organisation's ISP.

The next chapter concludes this study by summarising the findings as well as proposing recommendations for future research.

Chapter 8 : Conclusion and Recommendations

8.1 INTRODUCTION

This chapter concludes this study by revisiting the research objectives in Section 8.2. The summary of the research findings is discussed in Section 8.3. The implications for theory and practice are then stated in Section 8.4. Section 8.5 reflects the research limitations and Section 8.6 identifies possible opportunities for future research. Section 8.7 concludes the chapter.

8.2 RESEARCH OBJECTIVES

As mention in earlier chapters, most information security studies about ISP compliance tend to focus on theory and offer little or no practical effectiveness (Puhakainen and Siponen, 2010). There is paucity of empirical studies on behavioural information security and theoretical models which explain how awareness training affects behaviour (Puhakainen & Siponen, 2010 and Waly *et al*., 2012), which justifies the purpose of this study. This study therefore proposed a model based on the TPB to investigate the influence of ISP awareness training on end-user attitude towards complying with an organisations' ISP. The theory-based model was used to assess the factors contributing to ISP compliance. The model was then empirically validated using data collected from end-users of a single government organisation in one province. The results were then analysed and interpreted as shown in the previous chapter, whereas the conclusions drawn from the findings are further discussed in this chapter. The following section reiterates the objective of this study.

The main objective of this study was to investigate the influence of ISP awareness training on end-user attitudes towards complying with their organisation's ISP. The research sub-objectives formulated were:

- *To determine the current end-users level of ISP awareness training and ISP compliance behaviour.*
- *To assess the influence of ISP awareness training on end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP.*

8.3 SUMMARY OF THE RESEARCH FINDINGS

To achieve the main objective, the following research questions were inquired:

- *What is the current level of the end-user's ISP awareness training and their ISP compliance behaviour?*
- *How does ISP awareness training influence end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP?*

To answer these research questions, a literature review was conducted to gain knowledge of the underlying theory and the antecedents on which the different variables are built. Items based on the theory from previous studies were adopted to gather the information that enabled us to answer these questions and test the hypotheses**.**

The first research question yielded information about the current level of the end-users' ISP awareness training and their ISP compliance behaviour, whilst the second research question produced 5 hypotheses assessing how ISP awareness training influences end-users' attitudes toward ISP compliance and in turn their intention to comply with their organisation's ISP. In order to answer these research questions, a review of literature was conducted to understand the factors proposed to affect the intentions to comply in this study. Consequently a model based on the TPB with hypotheses was then proposed and tested, and it was found that 3 out of 5 hypotheses were supported. The following section summarises the findings of the research questions.

8.3.1 Summary of the first research question

The aim of the first research question was to determine the level of end-users' ISP awareness training in order to establish their existing knowledge regarding the information security policy of their organisation and make inferences about their current level of compliance towards it.

On the entire questionnaire regarding the current level of ISP awareness training, the results show that end-users know and understand their organisation's ISP, as the majority of the responses reflected negatively on the contradicting statement about the end-user's tendency to comply with the ISP when it is convenient to do so. Thus

we can conclude that end-users are not just aware of their ISP but understand and tend to comply with it.

However, the findings show that more can be done in terms of management organising information security training, and updating end-users on the changes related to the organisation's ISP. From the above findings, it can be inferred that the organisation's current information security culture needs to be improved in terms of organising and promoting ISP awareness training by management.

According to Hu, Dinev, Hart and Cooke (2012), management participation strongly influences organisational culture, which in turn impacts employees' attitudes and perceived behavioural control towards compliance with ISPs. Da Veiga (2015) furthermore suggests that, by encouraging effective information security awareness and training at all levels in an organisation, a positive information security culture can be promoted to enhance protection of information, minimise risk and contribute to compliance. From the above discussion, it can be inferred that management support and understanding the role of culture is fundamental to the successful implementation of information security.

8.3.2 Summary of the second research question

The objective of this research question was to assess how change on end-users' attitudes toward complying with their organisation's ISP is influenced by ISP awareness training. This research question yielded 5 hypotheses comparing three variables: ISP awareness training, attitude, self-efficacy and intentions to comply. The results of the hypotheses are as follows:

H1: ISP awareness training directly influencing on end-users' attitudes toward complying with their organisation was found to be insignificant.

H2: ISP awareness training positively affecting end-users' self-efficacy to comply with their organisation's ISP was found to be significant.

H3: self-efficacy positively affecting end-users' attitudes toward complying with the ISP was found to be significant.

H4: self-efficacy has no significant impact on end-users' intention to comply with the ISP.

H5: attitude towards complying with the organisation's ISP has a significant impact on their intention to comply.

The outcome of the hypotheses shows that end-users' attitudes could be indirectly altered by belief sets (self-efficacy). Since self-efficacy plays a role in determining how individuals feel, and think about their capabilities regarding compliance behaviour, which ultimately affects their behaviour (Fishbein and Ajzen, 1975; Bandura, 1977). It can therefore be established that, attitudes as targets of change can be altered by self-efficacy through awareness training, which will in turn create a security conscious culture within an organisation.

Furthermore, although the difference of the demographic variable (location) in terms of above hypotheses is not hypothesised in this study, this was also established and concluded on in this chapter as follows:

The mean difference of attitudinal by location

It was found that, there was no significant attitudinal difference found among the end-users of the three locations. In other words ISP awareness training did not significantly improve end-users' attitudes toward complying with the ISP in all the locations. These results imply that ISP awareness training in this study did not directly influence attitudes in all three locations.

The mean difference of self-efficacy by location

End-users self-efficacy about complying with the ISP showed improvement after the ISP awareness training intervention in all three locations, implying that the intervention had an effect on the end users' self-efficacy in all three locations.

The mean difference of intention to comply by location

Potchefstroom results suggested that participants are likely to follow the organisation's ISP in the future. However for Zeerust and Mafikeng, the results show that the intervention may not have improved the end-users' likelihood to follow the organisation's ISP in the future. The possible reason for this finding could be because the sample sizes for both Mafikeng and Zeerust might have been

insufficient to draw conclusions from separately, as compared to Potchefstroom which had a relatively large sample.

8.4 IMPLICATIONS FOR THEORY AND PRACTICE

According to Sommestad *et al*. (2014), achieving ISP in organisations is far from trivial. Waly *et al*. (2012) suggest that organisations should aim to investigate effective training and awareness techniques that will enhance employees' perceptions, attitude and motivation by transferring skills and sustaining appropriate behaviour toward information security. Having investigated the influence of ISP awareness training on end users' attitudes towards ISP compliance in this study, the following theoretical and practical implications are discussed:

8.4.1 Theoretical Implications

This study offers the following theoretical implications for scholars:

By including the survey on the level of awareness training and current compliance behaviour of the end-users, this research broadens knowledge regarding IS practices and behaviours in a government setting. These views are necessary for enhancing insight into information security practices in government organisations.

Furthermore, this study provides further empirical support to the findings in the existing literature, showing that self-efficacy can have an effect on attitude, which in turn should have a positive impact on ISP compliance behavioural intentions. Thus, the moderating effects of self-efficacy on attitudes are an important discovery and contribution on the application of ISP awareness training. Consequently, this discovery shed light on how attitudes can be influenced positively towards compliance behaviour.

8.4.2 Practical Implications

This study offers the following practical implications for information security practitioners:

As demonstrated by our supported research model, ISP awareness training positively affects end-users' self-efficacy, as with every increase of one unit in self-efficacy, attitudes were found to increase. Moreover, given the significant effect of

self-efficacy on attitudes towards ISP compliance and in turn intention to comply, it is recommended that practitioners could attempt to create ISP awareness training methods, such as incorporating videos with training (awareness training), thereby increasing end-users' belief sets (self-efficacy) about complying with the ISP, which will eventually have a positive effect on their attitudes and in turn their intentions to comply with the organisation's ISP. According to Tipton and Krause (2011), if you can subtly or directly change someone's attitude, you can consequently change behaviour. Thus, those lacking proper attitudes related to ISP compliance could benefit from such regular ISP awareness training interventions, as an individual's ISP compliance behavioural intention can be influenced by the attitude they have toward complying with the ISP.

Given the importance of self-efficacy on end-users' attitude toward ISP compliance, management could support and encourage end-users in developing the necessary skills and knowledge required to help safeguard organisational assets. Such encouragements will make it easy for ISPs and guidelines to be followed. As shown in the survey findings of this study, the need exists for managers to ensure that end-users are aware of the organisation's ISP and the potential damage that non-compliance could cause.

8.5 LIMITATIONS

- Since the sampling frame in this study was unknown, and the sample was not chosen at random, the inherent bias in convenience sampling means that the sample is unlikely to be representative of the population being studied. This undermines the researcher's ability to make generalisations from the sample obtained, to the population being studied. And since the sample in this study was obtained from a single government organisation in one province, the views collected from the participants cannot be generalised to other provinces or other government organisations.
- The data used in this study was collected at one point in time (cross-sectional), i.e. the effect of the experiment was measured right after the intervention was administered.
- The focus of the study was only on the awareness training level on the (NIST, 1998) learning continuum, thus role-based training and education were not

considered as they related to one's roles and responsibilities relative to IT systems and one's education and experience.

- The subjective norms were excluded in this study as they have been found to produce low meta-analysis when used with the other TPB constructs. According to Ajzen (2005), not all TPB constructs need to be significant to successfully explain intentions, as the relative importance of the three constructs is likely to change depending on the area of interest and the population being studied. Thus it is not clear whether the findings of the current study are unique or can be generalised to other settings.
- Furthermore, the use of intention as the dependent variable in this study raises the question of whether intention leads to actual behaviour. The rationale for the use of intention as the dependent variable in this study is that literature suggests that the best predictor of behaviour is intention (Fishbein and Ajzen, 1975). Moreover, measures of intention in studies exploring the relationship between intention and actual behaviour suggest a strong relationship between the two (Fishbein and Ajzen, 1975; Tipton and Krause, 2011; Sommestad *et al*., 2014). Thus the stronger the intention to carry out the behaviour, the more likely the behaviour is to be carried out (Fishbein and Ajzen, 1975). According to Crossler *et al*. (2013) and Waldo and Mathias (2016), collecting actual security behaviours is a challenge, hence many behavioural information security studies focused on capturing employees intentions instead (Bulgurcu *et al*., 2010; Ifinedo, 2012; Crossler *et al*., 2013; Waldo and Mathias, 2016). Therefore the researcher acknowledge that, although there is a lack of actual behaviour measurement after the intervention in this study, the measurement of intention is a valuable approximation that yields important insight into information security policy compliance research.

The discussed limitations incite avenues for future research presented in the next section.

8.6 FUTURE RESEARCH

- In order to improve the representativeness of future studies, it is suggested that probability sampling should be used to ensure that the sample being

studied is representative of the population of interest. Also, researchers should conduct further research on the influence of ISP awareness training on end-users' attitudes toward ISP compliance studies in a broader context, e.g. by including all provinces and or diverse government organisations, the data collected will be more representative. Moreover, future research in the context of the private sectors can be explored to compare the challenges of end-users' compliance with ISP in organisations and the impact ISP awareness training would have in different settings and/or cultures (i.e. research comparing private vs. public sector can be performed to investigate the model's viability).

- Research into the understanding of attitudes as targets of change to create more influential security awareness programmes can be studied further to determine the phenomenon of influence over time (a longitudinal study). This will be beneficial to determine if the changes found in attitudes persist over time or diminish once the study has been completed.
- Research focusing in role-based training and education could yield important insights into information security practices of Information Technology and security professionals to determine whether education and experience in IT has an effect on ISP compliance behaviour.
- Furthermore, future investigations could be conducted to examine whether the subjective norms are significant predictors of intention and actual ISP compliance behaviour when combined with other TPB constructs.
- Since there is a lack of actual behaviour measurement before and after the intervention in this study, action research about ISP compliance could also be beneficial. According to Frabutt, Holter and Nuzzi (2008) and Holter and Frabutt (2011), action research enables a researcher to develop a systematic inquiring approach toward their own practices or organisations focusing towards realising positive change in the organisation or in that practice. This kind of research could provide a researcher with an opportunity to measure end-users' actual compliance with their organisations' ISP objectively and yield valuable ISP awareness training and compliance behaviour information.

8.7 CONCLUSIONS

Government organisations are required to protect and safeguard sensitive information in response to compliance with statutory and regulatory requirements. Hence the “MISS” was approved as a national information security policy standard, intended to guide all government departments on information security (Basani, 2012). However the implementation of methods that aims to ensure compliance to information security policies have been found to be less than effective in influencing information security compliance behaviour. Thus, this study proposed a theory-based model to investigate how knowledge and skills, provided through ISP awareness training could influence end-users attitude toward complying with their organisation’s ISP.

According to Abawajy (2014), different training methods change our attitude towards certain issues. Furthermore, information security awareness of risks influences users’ attitude towards behaviour (Bryce and Fraser, 2014). Moreover, it is the responsibility of management to ensure that employees are aware of security risks and are trained on how to apply measures prescribed in the ISPs to protect information.

This study revealed that ISP awareness training has a significant influence on self-efficacy, which in turn has an influence on attitude and ultimately affects intentions to comply with the ISP. The implications discussed in this chapter will assist government organisations in implementing information security methods that are beneficial to end-users’ ISP compliance behaviour.

LIST OF REFERENCES

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Behaviour and Information Technology,* 33(3), pp. 237-248.

Adams, K. A. and Lawrence, E.K., 2015. *Research Methods, Statistics and Applications.* Sage Publications, Inc.

Ajzen, I., 1991. The theory of planned behaviour. *Organisational behaviour and human decision processes*, *50*(2), pp.179-211.

Ajzen, I., 2002. Constructing a TPB questionnaire: Conceptual and methodological considerations. [Online] Available from: http://chuang.epage.au.edu.tw/ezfiles/168/1168/attach/20/pta_41176_7688352_57138.pdf (Accessed on 10/10/2014)

Ajzen, I., 2005. *Attitudes, personality, and behaviour.* McGraw-Hill International.

Ajzen, I., 2011. The theory of planned behaviour: reactions and reflections. *Psychology & health*, *26*(9), pp.1113-1127.

Ajzen, I. and Timko, C., 1986. Correspondence between health attitudes and behavior. *Basic and Applied Social Psychology*, *7*(4), pp.259-276.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J. and Aleassa, H., 2013, "Information Security Policy Compliance: An Empirical Study of Ethical Ideology", *System Sciences (HICSS), 2013 46th Hawaii International Conference on* IEEE, , pp. 3018-3027.

Armitage C. J., and Conner, M., 2001. Efficacy of the theory of planned behaviour: A meta-analytic review*. British Journal of Social Psychology* 40(4), pp. 471-499.

Babbie, E.R., 2014. *The basics of social research*. Wadsworth, Cengage Learning.

Babbie, E., and Mouton, J., 2010. *The practice of social research*. Cape Town: Oxford University Press.

Bandura, A. 1977, "Self-efficacy: toward a unifying theory of behavioural change.", Psychological *review,* vol. 84, no. 2, pp. 191.

Basani, M., 2012. Towards A Framework To Ensure Alignment Among Information Security Professionals, ICT Security Auditors And Regulatory Officials In Implementing Information Security In South Africa. Master's Dissertation, University of South Africa. Available from http://uir.unisa.ac.za/handle/10500/9300 (Accessed 26/05/2013).

Barton, K.A. 2014. *Information System Security Commitment: A Study of External Influences on Senior Management.* Doctoral dissertation. Nova South Eastern University. [Online] Available from: http://nsuworks.nova.edu/gscis_etd/19 (Accessed on 10/04/2016)

Bishop, M., and Nascimento, A.C. eds., 2016. *Information Security: 19th International Conference, ICS 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings,* Springer.

Bollen, L.A., 1989. *Structural equations with latent variables.* New York: Wiley.

Boshoff, R., 2010. A baseline information security body of knowledge for end-users. *South African Information Security Multi- Conference (SAISMC) Postgraduate Symposium.* 17-18 May 2010

Bryce, J. and Fraser, J., 2014. The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behaviour,* 30, pp. 299-306.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2009. Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance, *Proceedings of the Fifteenth Americas Conference on Information Systems* 2009, pp. 1-9.

Burns, A. C. and Bush, R. F., 2010. *Marketing research.* Sixth Edition. Pearson.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security compliance: An Empirical Study of Rationally-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), pp. 523-548.

Cattel, R.B., 1978. *The scientific use of factor analysis.* New York: Plenum

Chan, K. and Gogoi, P., 2011. Hackers nab card data from 200,000 Citi customers. *Cnsnews.* [Online] *Available from*: *http://www.cnsnews.com/news/article/hackers-nab-card-data-200000-citi-customers* (Accessed on 10/07/2015)

Chakraborty, P. and Raghuraman, K., 2013. 'Trends in Information Security'. In: Khalid A. B. and Zaman, N. *Software Development Techniques for Constructive Information Systems Design*. IGI: Global. pp. 354-376.

Chawla, D. and Sodhi N., 2015. *Research Methodology: Concept and Cases*, second edition. VIKAS publishing house PVT LTD.

Cohen, L., Manion, L. & Morrison, K., 2011. *Research Methods in Education*. 7th ed. New York, USA: Routledge.

Compeau, D. R., Higgins C. A., 1995. Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly* 189-211.

Comrey, A.L. and Lee, H. B., 1999. *A first course in factor analysis*. Hillside, NJ:Erlbaum.

Corder, G.W., and Foreman, D.I., 2014. *Nonparametric statistics: a step-by-step approach.* John Wiley and Sons.

Cornford T., S. Smithson, 2006. *Project research in information systems: a student's guide*. Palgrave.

Creswell J. W. 2014. *Research design: A Qualitive, quantitive and mix method approaches.* Fourth Edition .Thousand oaks. Sage Publications Inc..

Crossler, R.E., Johnston, A.C., Lowry, P.B., HU, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioural information security research. *Computers & Security,* 32, pp. 90-101.

Davis, J., 2015. Hacking of Government Computers Exposed 21.5 Million People. *New York Times.* [Online] Available from: http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0 (Accessed on 30/11/2016)

Da Veiga, A. and Martins, N., 2014. Information Security Culture: A Comparative Analysis of Four Assessments, In *Proceedings of the 8th European Conference on IS Management and Evaluation (ECIME), University of Ghent, Belgium, 11-12 September 2014*, pp. 49-57.

Da Veiga, A., Martins, N. and Eloff, J.H., 2007. Information security culture–validation of an assessment instrument. *Southern African Business Review*, *11*(1), pp.147-166.

Da Veiga, A., 2015. An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security Positive Culture, In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*

D'arcy, J., Hovav, A. and Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research,* 20(1), pp. 79-98.

De Muth J. E., 2014. *Basic Statistics and Pharmaceutical Statistical Applications,* Third Edition, Chapman and Hall

De Vaus D.A., 2001. *Research Design in Social Research.* Sage Publications.

Dinev, T. and Hu, Q., 2007.The centrality of awareness in the formation of user behavioural intention toward protective information technologies. *Journal of the Association for Information Systems* 8(7), pp. 386–408.

Dishman R. K., R. W. Motl, R. Saunders, G. Felton, D. S. Ward, M. Dowda, R. R. Pate, 2005. Enjoyment mediates effects of a school-based physical-activity intervention*. Med.Sci.Sports Exerc.* 37(3), pp. 478-487.

Dugard, P., Todman, J.B. and Staines, H., 2010. *Approaching multivariate analysis: A practical introduction.* Routledge.

DPSA article 159. [Online] Available from: http://www.dpsa.gov.za/article.php?id=159 (Accessed on 15/07/2016)

Field A., G. Hole, 2002*. How to design and report experiments*. Sage.

Fishbein, M. and Ajzen, I., 1975. *Belief, attitude, intention and behavior: An introduction to theory and research.* Reading, MA: Addison - Wesley.

Fishbein, M. and Ajzen, I., 2005. The influence of attitudes on behaviour. *The handbook of attitudes,* pp. 173-222.

Frabutt, J. M., Holter, A. C., and Nuzzi, R. J., 2008. *Research, action, and change: Leaders reshaping Catholic schools*. Notre Dame, IN: Alliance for Catholic Education Press.

Ghaffari M., G. Sharifirad, E. Malekmakan, A. Hassanzadeh, 2013. Effect of educational intervention on physical activity-related knowledge, attitude and behaviour of among first-grade students of male high schools. *J.Educ.Health.Promot.* 2 4-9531.106642. eCollection 2013.

Ginsberg, L.H., 2001. *Social work evaluation: principles and methods*. Boston: Allyn and Bacon.

Grimes, R. A., 2015. 10 Years on: 5 big Changes to Computer Security. *CSonline.* [Online] Available from: https://www.CSonline.com/article/2972020/security/10-years-on-5-big-changes-to-computer-security.html. (Accessed on 10/11/2016)

Groebner D.F., Shannon P.W., Fry P.C. and Smith K.D., 2011. *Business Statistics A decision-making approach International Edition*, Eighth Edition Pearson Education Limited

Guilford, J.P. 1954. *Psychometric Methods*, 2nd edition. New York: McGraw Hill.

Haeussinger, F., 2013. Understanding the Antecedents of Information Security Awareness-An Empirical Study.

Hair, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C., 1995. *Multivariate data analysis.* New York: Macmillan Publishing Company.

Hair J.F. Jr, Black W.C., Babin B.J. and R.E., Anderson, 2014. *Multivariate Data Analysis,* 7th edition, Pearson Educated Limited, Essex, England

Hanafi S., H. Torkamandi, A. Hayatshahi, K. Gholami, N. A. Shahmirzadi, M. R. Javadi, 2014. An educational intervention to improve nurses' knowledge, attitude,

and practice toward reporting of adverse drug reactions. *Iranian Journal of Nursing and Midwifery Research* 19(1), pp. 101.

Heavey, E., 2014. *Statistics for nursing: A practical approach.* Jones and Bartlett Publishers.

Herath, T. and Rao, H., 2009. Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2), pp. 154-165. [Online] Available from: http://doi.org/10.1016/j.dss.2009.02.005 (Accessed on 17/08/2013)

Herold, R., 2010. *Managing an information security and privacy awareness and training program.* CRC Press.

Hockenbury, D., Hockenbury, S. E., 2007. *Discovering Psychology*. New York, NY: Worth Publishers.

Hofstee, E., 2006. *Constructing a good dissertation: A practical guide to finishing a master's MBA or PHD on schedule.* Johannesburg: EPE.

Holter, A. C., and Frabutt, J. M., 2011. *Action research in Catholic schools: A step-by-step guide for practitioners.* (2nd ed.). Notre Dame, IN: Alliance for Catholic Education Press.

Hovland, C.I. and Rosenberg, M.J., 1960. *Attitude organisation and change.* Yale University Press.

Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organisational culture. *Decision Sciences*, *43*(4), pp.615-660.

Humaidi, N. and Balakrishnan, V., 2013a. Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Journal of Health and Medical Informatics*.

Humaidi, N. and Balakrishnan, V., 2013b. Management Support as a Predictor to Promote Information Security Behaviour among Employees.

Hutcheson, G.D., and Sofroniou, N., 1999. *The Multivariate Social Scientist Introductory Statistics Using Generalized Linear Models.* Sage Publications LTD.

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behaviour and the protection motivation theory. *Computers and Security,* **31**(1), pp. 83-95.

Ifinedo, P., 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management,* **51**(1), pp. 69-79. [Online] Available from: http://doi.org/10.1016/j.im.2013.10.001 (Accessed on 19/03/2016)

ISO/IEC 27001, 2013. Information technology — Security techniques — Information security management systems Requirements. International Organisation for Standardization. [Online] Available from: http://www.iso27001security.com/html/27001.html (Accessed on 10/10/2015)

ISO/IEC 27002, 2013. Information technology — Security techniques — Code of practice for information security controls. International Organisation for Standardization. [Online] Available from: http://www.iso27001security.com/html/27002.html (Accessed on 10/10/2015)

ISO/IEC 27003, 2010. Information technology — Security techniques — Information security management system implementation guidance. International Organisation for Standardization. [Online] Available from: http://www.iso27001security.com/html/27003.html (Accessed on 10/10/2015)

ISO/IEC 27004, 2009. Information technology — Security techniques — Information security management — Measurement. International Organisation for Standardization. [Online] Available from: http://www.iso27001security.com/html/27004.html (Accessed on 10/10/2015).

Jacobsen, K.H., 2012. *Introduction to Health research methods: A practical guide*. Jones and Bartlerr Learning,LLC.

Johnson, N., 2015. 'Staggering' Hack of Government Computers Exposes 21.5 Million People, Forcing Director's Resignation. *The Daily Signal.* [Online] Available

from: http://dailysignal.com/2015/07/10/staggering-hack-of-government-computers-exposes-21-5-million-people-forcing-directors-resignation/ (Accessed on 24/02/2016).

Johnson R. and Kuby P., 2012. *Elementary Statistics,* 11th Edition Brooks, CENGAGE learning

Kaiser, H. F., 1960. The application of electronic computers to factor analysis. *Educational and Psychological Measurement, 20*, pp. 141-151.

Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K., 2011. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management,* 5(26), pp. 10862-10868.

Kim, S.H., Yang, K.H. and Park, S., 2014. An integrative behavioural model of information security policy compliance. *The Scientific World Journal,* 2014, pp. 463870.

King, S. and Hart, D., 2009. Public Sector vs Private Sector. Who does security better? Part 1-4. [Blog] *Risk Management with Stuart King and Duncan Hart*. Available from: http://itknowledgeexchange.techtarget.com/risk-management/page/3/ [Accessed 16 Oct. 2016].

Kline, P., 1994. *An Easy Guide to Factor Analysis*. New York: Routledge

Knapp, J., Ferrante, C.J., 2012. Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organisations. *Journal of Management Policy and Practice*, 13(5), pp. 66-80.

Kumar R., 2014. *Research methodology: A step by step for beginners*. Sage.

Kumar S. and Phrommathed, P., 2005*. Research methodology*. Springer.

Leary, M., 2012. *Introduction to Behavioural research Methods*. Sixth Edition. Pearson Education Inc.

Levine, D.M. Krehbiel, T.C and Berenson, M.L., 2013. *Business Statistics A first Course*, Sixth Edition, Pearson Educated Limited, USA.

Levine, D.M., Szabat, K. A. and Stephan D.F., 2016. *Business Statistics A first Course*, Seventh Edition, Pearson Educated Limited, USA.

Li, L.K., 2012. A study of the attitude, self-efficacy, effort and academic achievement of CityU students towards research methods and statistics. *Discovery–SS Student E-Journal,* 1(2), pp. 154-183.

MacCallum, R.C., Browne, M.W. and Sugawara, H.M.,1999. Power analysis and determination of sample size in covariance structure modelling. *Psychological Methods,* 1, pp. 130-149.

Maio, GR, and Haddock, G, 2010. *The psychology of attitudes and attitude change.* London: Sage Publications Ltd.

Manikandan S., 2011. Measures of central tendency: Median and mode. *J Pharmacol Pharmacother*, 2(3), pp.214-215. doi: 10.4103/0976-500X.83300.

Marano, P., Rokas, I. and Kochenburger, P. eds., 2016. *The" Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective*. Springer.

Martin N. and Rice J. 2011. Cybercrime: understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), pp. 803-814.

Mattord H. J., M. E. Whitman., 2008. Principles of information security*. Thomson Course Technology,[13] SITE.(Nd),"The Search for International Terrorist Entities".* [Online] Available from: Http://www.Siteinstitute.Org/.Boston, *MA, Appendix* 326. (Accessed on 31/03/2014).

Mavetera, N., Makhudu, A.B., 2012. Investigating Information System Security Policy and Awareness Training Programs in South African Organisations. 20th IBIMA Conference, 12-13 November 2012, Barcelona, Spain.

McEachan, R.R.C., Conner, M., Taylor, N.J. and Lawton, R.J., 2011. Prospective prediction of health-related behaviours with the theory of planned behaviour: A meta-analysis. *Health Psychology Review*, *5*(2), pp.97-144.

Merhi, M.I. and Midha, V., 2012. The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study. [Online] Available from:

http://aisel.aisnet.org/icis2012/proceedings/ResearchInProgress/73/ (Accessed on 10/10/2015)

Mertens, D.M., 2009. *Transformative research and evaluation*. New York: The Guilford Press.

Minimum Information Security Standards, 1998. 2nd edition. [Online] Available from: http://www.right2info.org/resources/publications/laws_1/SA_Minimum%20Information%20Security%20Standards.pdf. (Accessed on 16/11/2012).

Monette, D.R., Sullivan, T.J. and Dejong, C.R., 2011. *Applied social research: a tool for the human services.* New York: Brooks/Cole Cengage Learning.

Moser, G., Uzzell, D., Millon, T. and Lerner, M., 2003. Comprehensive Handbook of Psychology.

National Strategic Intelligence Act 39 of 1994. [Online] Available from:http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/National%20Strategic%20Intelligence%20Act%2039%20of%201994.pdf (Accessed on 30/10/2016)

NIST, 2003. *Building an Information Technology Security Awareness and Training Program.* National Institute for Standards and Technology Special Publication 800-50. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf. (Accessed on 10/12/2014).

NIST, 2009. *Information Security Training Requirements: A Role- and Performance-Based Model*. National Institute for Standards and Technology Special Publication No. 800-16 Revision 1 -Draf). (Accessed on 15/19/2013).

NIST, 1995. *An Introduction to Computer Security.* National Institute for Standards and Technology Special Publication 800-12. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf. (Accessed on 10/12/2014).

NIST, 1998. *Information Technology Training Requirements: A Role-and Performance-Based Model*. National Institute for Standards and Technology Special Publication 800-16. Washington, DC: US Department of Commerce.

Ng, B., Kankanhalli, A. and Xu, Y., 2009. Studying users' computer security behaviour: A health belief perspective. *Decision Support Systems*, 46(4), pp. 815.

Ngobeni, S.J. and Grobler, M., 2009. Information Security Policies for Governmental Organisations, the Minimum Criteria. In *ISSA* (pp. 455-466).

Ngoma, S., 2012. Vulnerability of IT Infrastructures: Internal and External Threats. [Online] Available from: http:/www.congovision.com/IT-Security-Pub.pdf

Nkwana, M.J., 2015. *The Protection of Security Information within Government Departments in South Africa*. Master's Dissertation, University of South Africa. [Online] Available from: http://hdl.handle.net/10539/7421 (Accessed 26 August 2016).

Nunnally, J. C., 1967. *Psychometric Theory*, New York: McGraw-Hill.

Oates, B. J., 2006. *Researching information systems and computing.* London: Sage Publications Ltd.

Pallant J., 2010. *SPSS Survival Manual: A step by step guide to data analysis using SPSS.* McGraw-Hill Education

Pahnila, S., Siponen M. and Mahmood A., 2007. 'Employees behaviour towards IS Security Policy Compliance'. *Proceedings of the 40th Hawaii International Conference on System Sciences*, IEEE, pp. 156-166.

Parahoo, K., 2014. *Nursing research: principles, process and issues*. Palgrave Macmillan.

Pearson, R. H. and Mundform, D. J. 2010. Recommended Sample Size for Conducting Exploratory Factor Analysis on Dichotomous Data. *Journal of Modern Applied Statistical Methods*. 9(2), pp.359-368. [Online] Available from: http://digitalcommons.wayne.edu/jmasm/vol9/iss2/5 (Accessed on 01/05/2015).

Peltier, T.R., 2014. *Information Security Fundamentals*. Second Edition. CRC Press/Taylor and Francis.

Peltier, T.R. 2016, *Information Security Policies, Procedures, and Standards: guidelines for effective information security management,* CRC Press.

Pierson, J. and Thomas, M., 2010. *Dictionary of social work: the definitive A to Z of social work and social care*. New York: McGraw Hill Open University Press.

Ponemon Institute and Raytheon Release New Study on the Insider Threat. (2014). [Blog] *Ponemon Institute*. [Online] Available from: http://www.ponemon.org/blog/ponemon-institute-and-raytheon-release-new-study-on-the-insider-threat (Accessed on 13/09/2016).

Protection of Information Act 82 of 1982. Government Gazette 32999. Pretoria: Government printer. [Online] Available from: https://www.gov.za./documents/protection-information-act-20-mar-2015-1202. (Accessed on 10/09/2016).

Public Service Act 103 of 1994. Government Gazette 32999. Pretoria: Government printer. [Online] Available from: https://www.dpsa.gov.za/acts&regulations/psact1994/PublicServiceAct.pdf. (Accessed on 10/09/2016).

Puhakainen P., M. Siponen. 2010. Improving employees' compliance through information systems security training: An action research study. *Mis Quarterly* 34(4), pp. 757-778.

Raduege Jr, H.D., 2013. The Public/Private Cooporation We need on Cyber Security. [Online] Available from: https://hbr.org/2013/06/the-publicprivate-cooperation (Accessed on 13/11/2016).

Raggad, B.G., 2010. *Information security management: concepts and practice*, Boca Raton, FL: CRC Press/Taylor and Francis.

Rastogi, R. and von Solms, R., 2011. Information Security Service Support-Helping End-Users Cope with Security. *Computer Technology and Application* **2**, pp. 137-147

Remler, D. K. and Van Ryzin, G. G., 2011. Research methods in practice: strategies for description and causation. Thousand Oaks, Califonia: SAGE Publications

Revelle, W. and Zinbarg, R., 2009. Coefficients Alpha, Beta, Omega, and the glb: Comments on Sijtsma. *Psychometrika,* 74(1), pp. 145-154.

Rezaei, M., Zamani-Miandashti, N. and Shiraz, I., 2013. The relationship between research self-efficacy, research anxiety and attitude towards research: A study of agricultural graduate students. *Journal of Educational and Instructional Studies in the World,* 3(4), pp. 69-78.

Ritchey, D., 2010. Public and Private Security: Bridging the Gap. *Security Magazine.* [Online] Available from: http://www.securitymagazine.com/articles/80710-public-and-private-security-bridging-the –gap-1 (Accessed on 11/05/2015)

Rossi, B., 2016. Five years in information security what has changed. [Online] Available from: http://www.information-age.com/five-years (Accessed on 30/11/2016)

Safa, N.S., Sookhak, M., Von Solms, R., FurnelL, S., Ghani, N.A. and Herawan, T., 2015. Information security conscious care behaviour formation in organisations. *Computers and Security,* **53**, pp. 65-78.

Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organisations. *Computers and Security,* **56**, pp. 70-82.

Salkind N.J., 2012. *Exploring Research*. Eighth Edition, Pearson Education, Inc.

Sapsford, R., 2006. *Survey research.* Sage.

Saunders, M., Lewis, P. and Thornhill, A., 2009. *Research Methods for Business Students,* 5th ed., UK: Pearson Education.

Schumacker R.E. and Lomax R.G., 2010. *A beginner's guide to structural equation modelling*, Third Edition, Routledge Taylor and Francis Group, USA

Sentosa I., N. Mat, 2012. Examining a theory of planned behaviour (TPB) and technology acceptance model (TAM) in internet purchasing using structural equation modeling*. Journal of Arts, Science and Commerce* **3**(2), pp.62-77.

Sharma, R. and Gupta, M., 2009. *Handbook of Research on Social and Organisational Liabilities in Information Security.* Hershey, PA, USA: IGI Global.

Shaw, T.J., 2012. *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists*. American Bar Association.

Sheeran P., 2002. Intention—behaviour relations: A conceptual and empirical review*. European Review of Social Psychology* **12**(1), pp.1-36.

Siponen M., M. A. Mahmood, S. Pahnila, 2014. Employees' adherence to information security policies: An exploratory field study*. Information and Management* **51**(2), pp. 217-224.

Siponen, M., and Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management* **46**(5), pp. 267-270.

Siponen, M. and Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly,* **34**(3), pp. 487.

Siponen, M., Pahnila, S. and Mahmood, M.A., 2010. Compliance with information security policies: An empirical investigation. *Computer,* 43(2), pp. 64-71.

Sommestad T., Hallberg J., Lundholm K., Bengtsson J., 2014. Variables influencing information security policy compliance: A systematic review of quantitative studies*. Information Management and Computer Security* **22**(1), pp. 42-75.

Soomro Z. A., Shah H.S. and Ahmed j., 2016.Information security management needs holistic approach: A literature review. *International journal of information management,* **22***,* pp. 215-225.

Spielberger, C., 2004. *Encyclopedia of Applied psychology.* Oxford, Boston : Elsevier Academic Press

Stangor, C., 2004. Research methods for the behavioral sciences. Second edition, Boston, Mass.: Houghton Mifflin.

Stangor, C., 2011. *Research methods for the behavioural sciences*. Fourth edition, Australia; Belmont, CA: Wadsworth Cengage Learning.

Stewart, J.M., Chappel, M., Gibson, D., 2015. *CISSP (ICS)2 Certified Information Security Professional Official Study guide.* 7th revised Edition. John Wiley & Sons Inc.

Sung, P. and Su, C., 2013. Using System Dynamics to Investigate the Effect of the Information Medium Contact Policy on the Information Security Management. *International Journal of Business and Management,* **8**(12), pp. p83.

Susanto, H. and Almunawar, M., 2012. Information Security Awareness: A Marketing Tools for Corporate's Business Processes. *Computer Science Journal, August*.

Susanto, H., Almunawar, M.N. and Tuan, Y.C., 2012. Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level. *International Journal of Engineering and Technology,* 2(1).

Tabachnick B.G. and Fidel L.S., 2014. *Using Multivariate Statistics.*6th Edition. Pearson Education Limited.

Takemura, T. and Komatsu, A., 2012. Who Sometimes Violates the Rule of the Organisations?: Empirical Study on Information Security Behaviours and Awareness, 2012, WEIS.

Thyer, B., 2010. *The handbook of social work research methods*. Los Angeles: Sage Publications.

Tipton, F. and Krause M., 2011. *Information Security Management Handbook,* Edition 6, Volume 5. Boca Raton: Auerbach Publications.

Tipton, F. and Krause M., 2012. *Information Security Management Handbook,* Edition 6, Volume 6. Boca Raton: Auerbach Publications.

Topa, G. and Moriano, J.A., 2010. Theory of planned behavior and smoking: Meta-analysis and SEM model. *Substance Abuse and Rehabilitation*, ***1***, pp.23-33.

Trochim, W.M., 2006. *Research methods knowledge base*. Sage.

Vance, A., Siponen, M. and Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, **49**(3), pp.190-198.

Waldo, R. F. and Mathias, E., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computer & Security,* **59**, pp 26-44.

Waly, N., Tassabehji, R. and Kamala, M., 2012. Improving organisational information security management: The impact of training and awareness, *High Performance Computing and Communication and 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on* 2012, IEEE, pp. 1270-1275.

Warkentin, M., Johnston, A.C. & Shropshire, J., 2011, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems,* 20(3), pp. 267-284.

Welman C., F. Kruger, B. Mitchell. 2005*. Research methodology*. Oxford University Press.

Whitman, M. and Mattord, H., 2011. *Principles of information security.* Cengage Learning.

Whitman, M. and Mattord, H., 2013. *Management of information security.* Cengage Learning.

Wolf, M., Haworth, D. and Pietron, L., 2011. Measuring an information security awareness program. *Review of Business Information Systems (RBIS),* **15**(3), pp. 9-22.

Wong, C., Odom, S.L., Hume, K.A., Cox, A.W., Fettig, A., Kucharczyk, S., Brock, M.E., Plavnick, J.B., Fleury, V.P. and Schultz, T.R., 2015. Evidence-based practices for children, youth, and young adults with autism spectrum disorder: A comprehensive review. *Journal of Autism and Developmental Disorders,* **45**(7), pp. 1951-1966.

LIST OF APPENDICES

APPENDIX A: REQUEST FOR PERMISSION

Telephone: Private Bag

SSN:

E-Mail:

Enquiries Ms M.Snyman 10 April 2014

Request for Approval:

Re: Research Study: The influence of information security awareness and training on end-user's attitudes towards Information Security Policy (ISP) Compliance.

To whom it may concern,

I am currently undertaking a Master's degree in IT (information security field) with UNISA. A research proposal regarding the study has been submitted and approved by the university as partial fulfilment of the course (proposal attached). The topic chosen is aimed at examining end-user's attitude towards ISP compliance and the influence awareness and training has on the subject.

I therefore wish to request your permission to invite North West Members who are registered on the network currently to participate in this study.

The information needed to complete this study will be gathered by means of a questionnaire, an example of which is included on the proposal. The results could prove to be beneficial in identifying issues relating to information security policy compliance that need to be addressed and to contribute to the information security practice in this era.

Should you agree to the members participating in this study, I will be grateful if I would be provided with the list of all North West province Users that are registered on the network. Confidentiality and anonymity will be assured at all times.

Thank you for taking the time to read this letter. If you have any queries or would like to discuss this matter further before making a decision, please do not hesitate to contact me on the telephone number provided.

Yours sincerely,

Mmabatho Snyman

APPENDIX B: LETTER OF AUTHORITY TO CONDUCT THE REASEARCH

April 2014

AUTHORITY TO CONDUCT A RESEARCH IN THE DOD MRS MMABATHO SNYMAN

1. Your submission as well as research proposal dd 10 April 2014 has reference.

2. Permission is hereby granted from a security perspective to Mrs M. Snyman to conduct the research entitled "**The influence of information security awareness and training on end user's attitudes towards Information Security Policy (ISP)"** as requested.

3. Authority is granted on condition that there will be no list of the network end users provided to the researcher and no details of the research subjects will be mentioned in the research end product which must be sent to before it's dispatched to University of South Africa.

Yours faithfully.

(Attention: Ms M. Snyman)

SENT BY POST 13/05/14
AU FAX NUMBER

APPENDIX C: ETHICAL CLEARANCE

UNISA | college of science, engineering and technology

Mrs Mmabatho Charity Snyman (50812300) 2014-08-25
College of Science, Engineering and Technology
UNISA
Johannesburg

Permission to conduct research project

Ref: 152/ MCS /2014

The request for ethical approval for your MTech (Information Technology) research project entitled "Awareness and Training: The influence on end user's attitude toward Information Security Policy (ISP) Compliance." refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

Prof Ernest Mnkandla
Chair: College of Science, Engineering and Technology Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
[illegible]
Florida Park, Roodepoort
[illegible]
www.unisa.ac.za/cset

UNISA | college of science, engineering and technology

APPENDIX D: INFORMED CONSENT

INFORMED CONSENT FORM FOR PARTICIPANTS

Title of Research Project:

Awareness Training: The Influence on end-user attitudes toward information security policy (ISP) compliance.

Investigator:

Name: Mmabatho Snyman

E-Mail:

Phone:

Cell:

Instructions:

Before filling out the survey questionnaire, please first read carefully and sign this "Informed Consent" Form. This form must be returned with the questionnaire in order for us to include your comments in our study. All information will be kept confidential and no names will be used.

Back ground:

I am currently undertaking a Master's degree with the University of South Africa (UNISA). The topic I have chosen aims to illustrate the influence of awareness training on end-users attitudes towards ISP compliance. In my experience as an ISS Specialist, I have observed different levels of awareness and compliance regarding ISP amongst end-users. This is a situation that needs to be addressed as end-users need to understand ISPs in order to comply with their organisation's ISP, Moreover users need to be appropriately trained in the rules of behaviour and must be aware of actions they can take to better protect their organisation's information. It is anticipated that the results of this study will generate information that will contribute to the effectiveness of ISP awareness training in improving end-user's attitudes and ultimately encourage end-user behaviour towards a more favourable state.

Before participating, you should know enough about the study to make an informed decision.

Study procedure:

Participation in this study involves the following:

Participants will complete a confidential questionnaire that consists of two sections. Section A consist of separate questions on demographics, behavioural and level of awareness questions, section B consists of pre-attitude, Self-efficacy and Intention to comply questionnaires, this questionnaire should only take ±30 minutes of your time to complete.

A percentage of the participants will receive a short presentation regarding ISP, followed by a short movie; this should take less than 1 hour. After which a post-attitude questionnaire will be provided for completion to measure the effect of awareness training by all participants again.

Risks:

There are no known risks associated with this research project other than possible discomfort with the following:

• You will be asked to be completely honest when completing the form.

• You will be asked to complete the questions independently without discussion with others to allow for more accurate results.

Benefits:

There are no monetary benefits, however possible benefits for participation in this project are:

• You will contribute knowledge about the information security policy compliance issues in organisations.

• You will help improve information security behaviour of end-users to better protect organisational information.

Alternative procedures:

Remember, participation is voluntary. You may choose not to participate, and you may withdraw at any time during the research project. You will NOT be penalized in any way should you choose not to participate or to withdraw.

We will do everything we can to protect your privacy. As part of this effort, your identity will not be revealed in any publications that result from this study. The information in the study

records will be kept strictly confidential. Research data will be stored securely and will be made available only to persons conducting the study. No reference will be made in oral or written reports that could link you to the study.

Contact person:

For any queries or concerns about the study or procedures, you may contact the researcher on the above mentioned details.

==========

I have read this consent form and I am willing to participate in the study.

Yes ☐ **No** ☐

I have been given the opportunity to ask questions and therefore grant permission to use the information I provide as data in the research project, knowing that it will be kept confidential and without use of my name.

Participant's Signature **Date**

_____ _____

I am also interested in receiving a summary of the research report when available:

Yes ☐ **No** ☐

If yes kindly provide your email address below.

_____

APPENDIX E: RESEARCH INSTRUMENT

Completion of this questionnaire must only be done if the participant has read the consent form and agreed by signature to participate in the study. You are further requested to complete the questionnaire as honestly and carefully as you can.

Section: A

Part 1: Demographics

Please answer each question by ticking only 1 the appropriate box per question.

1. Please indicate your gender

Male ☐ Female ☐

2. Please indicate how frequently you have been using a computer in your organisation.

Under 1 year	
1 - 3	
4 - 6	
7 - 9	
More than 10 years	

1. Please indicate your age in the box space provided below

2. Please indicate the number of years you have been with the organisation below.

3. Please indicate your work area by ticking in the appropriate box

Mafikeng ☐ Potchefstroom ☐ Zeerust ☐

SURVEY - QUESTIONNAIRE

SECTION A

The following measurement criteria is used:

	1 Strongly Disagree	**2** Disagree	**3** Neither Agree nor Disagree	**4** Agree	**5** Strongly Agree	

Please indicate your response by ticking the appropriate answer

LEVEL OF INFORMATION SECURITY POLICY AWARENESS TRAINING QUESTIONS

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
1. I am aware of potential information security threats.					
2. I keep myself updated in terms of information security awareness.					
3. I know the rules and regulations prescribed by the Information Security Policy of my organisation.					
4. I understand the rules and regulations prescribed by the Information Security Policy of my organisation.					
5. I know my responsibilities as prescribed in the Information Security Policy to enhance the IS security of my organisation.					
6. The management updates me on the changes related to the Information Security Policy.					
7. The management organises information security training effectively.					
8. The management encourages me to attend the information security trainings.					
9. Information Security Policy training in my organisation helps me to understand how to behave appropriately towards matters related to information security.					

CURRENT BEHAVIOURAL QUESTIONS

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
1. I comply with the Information Security Policy when performing my daily work.					
2. I tend to comply with the Information Security Policy only when it is convenient to do so.					
3. I practice recommended information security behaviour as much as possible.					
4. I assist others in complying with information security policy.					
5. I recommend others to comply with information security policy.					

PRE- EXPERIMENTAL QUESTIONNAIRE

SECTION B

The following measurement criteria is used:

	1 Strongly Disagree	**2** Disagree	**3** Neither Agree nor Disagree	**4** Agree	**5** Strongly Agree	

Please indicate your response by ticking the appropriate answer

EXPERIMENT QUESTIONNAIRE

ATTITUDINAL QUESTIONNAIRE

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
1. I feel that compliance to information security policies is a positive thing.					
2. I feel that compliance to information security policies is important.					
3. Following the organisation's ISP is a good idea.					
4. Information security policy helps secure computer systems.					
5. Following the organisation's ISP is a necessity.					

SELF-EFFICACY QUESTIONNAIRE

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
1. I have the necessary skills to fulfil the requirements of the ISP.					
2. I have the necessary knowledge to fulfil the requirements of the ISP.					
3. I can use information security measures if I can call for help if I get stuck.					
4. I have the necessary skills to protect myself from information security violations.					
5. I have the expertise to implement preventative measures to stop people from getting my confidential information.					
6. It is easy for me to enable security features on my work computer by myself.					
7. I believe that it is within my control to protect myself from information security violations.					

PLEASE TURN OVER THE PAGE TO CONTINUE!!!!

The following measurement criteria is used:						
	1 Strongly Disagree	**2** Disagree	**3** Neither Agree nor Disagree	**4** Agree	**5** Strongly Agree	
Please indicate your response by ticking the appropriate answer						

INTENTION TO COMPLY WITH THE INFORMATION SECURITY POLICY QUESTIONNAIRE					
*** Mark appropriate block with a X**					
	1	**2**	**3**	**4**	**5**
1. I intend to comply with information security policies.					
2. I intend to assist others in complying with information security policies.					
3. I am likely to follow the organisation's ISP in the future.					
4. I would follow the organisation's ISP whenever possible.					
5. I am certain I will adhere to my organisation's ISP.					

POST- EXPERIMENTAL QUESTIONNAIRE

SECTION B

The following measurement criteria is used:

	1 Strongly Disagree	**2** Disagree	**3** Neither Agree nor Disagree	**4** Agree	**5** Strongly Agree	

Please indicate your response by ticking the appropriate answer

EXPERIMENT QUESTIONNAIRE

ATTITUDINAL QUESTIONNAIRE

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
6. I feel that compliance to information security policies is a positive thing.					
7. I feel that compliance to information security policies is important.					
8. Following the organisation's ISP is a good idea.					
9. Information security policy helps secure computer systems.					
10. Following the organisation's ISP is a necessity.					

SELF-EFFICACY QUESTIONNAIRE

*** Mark appropriate block with a X**

	1	**2**	**3**	**4**	**5**
8. I have the necessary skills to fulfil the requirements of the ISP.					
9. I have the necessary knowledge to fulfil the requirements of the ISP.					
10. I can use information security measures if I can call for help if I get stuck.					
11. I have the necessary skills to protect myself from information security violations.					
12. I have the expertise to implement preventative measures to stop people from getting my confidential information.					
13. It is easy for me to enable security features on my work computer by myself.					
14. I believe that it is within my control to protect myself from information security violations.					

PLEASE TURN OVER THE PAGE TO CONTINUE!!!

The following measurement criteria is used:						
	1 Strongly Disagree	**2** Disagree	**3** Neither Agree nor Disagree	**4** Agree	**5** Strongly Agree	
Please indicate your response by ticking the appropriate answer						

INTENTION TO COMPLY WITH THE INFORMATION SECURITY POLICY QUESTIONNAIRE					
*** Mark appropriate block with a X**					
	1	**2**	**3**	**4**	**5**
6. I intend to comply with information security policies.					
7. I intend to assist others in complying with information security policies.					
8. I am likely to follow the organisation's ISP in the future.					
9. I would follow the organisation's ISP whenever possible.					
10. I am certain I will adhere to my organisation's ISP					

APPENDIX F: CERTIFICATE OF EDITING

Certificate of Language Editing

17 Strydom Street
Baillie Park
Potchefstroom
2531
20 February 2017

TO WHOM IT MAY CONCERN

I hereby confirm that I have read and edited the dissertation of Mmabatho Charity Snyman, entitled:

AWARENESS AND TRAINING: THE INFLUENCE ON END-USER ATTITUDE TOWARDS INFORMATION SECURITY POLICY COMPLIANCE

submitted in accordance with the requirements for the degree of **MAGISTER TECHNOLOGIAE** in Information Technology.

I have been proofreading dissertations and theses in various fields for more than twenty years.

I have only made a few minor adjustments to this dissertation, as it was thorough and well written. I trust the writing is on standard.

Yours sincerely

H. Krieg
henkrieg@gmail.com
0833679308